VERINT

Witness Actionable Solutions

IMPACT360™

Full-time Recorder

System Administration Guide

Release 7.8. SP1
January, 2008

© 2008 Verint Systems Inc. All Rights Reserved Worldwide.
Confidential and Proprietary Information of Verint Systems Inc.

The Verint Systems Inc. products are protected by one or more of the following U.S., European or International Patents: USPN 5,659,768; USPN 5,790,798; USPN 6,278,978; USPN 6,370,574; USPN 6,404,857; USPN 6,510,220; USPN 6,757,361; USPN 6,782,093; USPN 6,952,732; USPN 6,959,405; USPN 7,047,296; USPN 7,149,788; USPN 7,155,399; USPN 7,203,285; USPN 6,959,078; USPN 6,724,887; USPN 7,216,162; European Patent 0 833 489; GB 2374249; and other provisional rights from one or more of the following Published US Patent Applications: US 10/061,469; US 10/061,489; US 10/061,491; US 11/388,854; US 11/388,944; US 11/389,471; US 10/818,787; US 11/166,630; US 11/129,811; US 11/477,124; US 11/509,553; US 11/509,550; US 11/509,554; US 11/509,552; US 11/509,549; US 11/509,551; US 11/583,381; US 10/181,103; US 09/825,589; US 09/899,895; US 11/037,604; US 11/237,456; US 09/680,131; US 11/359,356; US 11/359,319; US 11/359,532; US 11/359,359; US 11/359,358; US 11/359,357; US 11/359,195; US 11/385,499; US 11/394,496; US 11/393,286; US 11/396,061; US 11/395,992; US 11/394,410; US 11/394,794; US 11/395,350; US 11/395,759; US 60/799,228; US 11/479,926; US 11/479,841; US 11/479,925; US 11/479,056; US 11/478,714; US 11/479,899; US 11/479,506; US 11/479,267; US 60/837,816; US 11/528,267; US 11/529,132; US 11/540,281; US 11/540,322; US 11/529,947; US 11/540,902; US 11/541,056; US 11/529,942; US 11/540,282; US 11/529,946; US 11/540,320; US 11/529,842; US 11/540,904; US 11/541,252; US 11/541,313; US 11/540,086; US 11/540,739; US 11/540,185; US 11/540,107; US 11/540,900; US 10/610,780; US 10/832,509; US 11/608,340; US 11/608,350; US 11/608,358; US 10/771,315; US 10/771,409. Other U.S. and International PatentsPending.

VERINT, the VERINT logo, ACTIONABLE INTELLIGENCE, POWERING ACTIONABLE INTELLIGENCE, STAR-GATE, RELIANT, VANTAGE, X-TRACT, NEXTIVA, ULTRA, AUDIOLOG, WITNESS, the WITNESS logo, IMPACT 360, the IMPACT 360 logo, IMPROVE EVERYTHING, EQUALITY, CONTACTSTORE, and CLICK2STAFF are trademarks or registered trademarks of Verint Systems Inc. or its subsidiaries. Other trademarks mentioned are the property of their respective owners.

Doc Version 7.8.1-2
2008-01-31

Contents

About This Guide 7

Intended Audience for This Guide 8
Summary of Information Included in This Guide 9
Related Documents 12
Conventions Used in This Guide 13
If You Need Help 15
Before You Contact Technical Support 15
Contacting Technical Support 16
Verint Witness Actionable Solutions Website and the Customer Interaction Center (CIC) 16
Telephone 16
Email 17
Direct internet FTP 17
Other support and training alternatives 17

Getting Started 19

Setting Up 20
Logging Into the System 20
Configuring the Recorder License 23
Creating Users 27
Using System Logs 30

Working with Components 37

Configuring Integration Service CTI Adapters 38
Configuring Adapter Settings 38
Configuring Adapter Custom Attributes 42
Configuring Common Components 46
Viewing the Recorder's Status 47
Setting up the Recorder 59
Configuring Archive 65
Configuring Disk Manager 77
Configuring Database Settings 79
Configuring IP Recording Components 84
Configuring Compression 84
Managing Extensions 86
Configuring Optional Components 93
Configuring Live Monitor and Observer 94

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Screen Recording . . . 105
Configuring Centralized Archiving . . . 106

Using Voice Cards, NICs and Analyzer . . . 109

Configuring Voice Cards . . . 110
Performing General Voice Card Tasks . . . 111
Configuring T1/E1 Voice Cards . . . 121
Configuring PCM32 Voice Cards . . . 129
Configuring NGX Voice Cards . . . 135
Configuring Cybertech Voice Cards . . . 142
Configuring Analog Voice Cards . . . 148
Voice Card Troubleshooting . . . 152
Configuring Network Interface Cards . . . 159
Configuring Network Settings . . . 159
Tutorial: Configuring Call Manager for Active Recording: . . . 166
Configuring Analyzer . . . 170
Viewing Analyzer . . . 171
Using Analyzer Manager . . . 173
Configuring Call Control . . . 177

Managing System Components . . . 183

Monitoring Components with Alarms . . . 184
Configuring Alarms . . . 185
Viewing and Monitoring Alarms . . . 191
Setting Alarm Notification Profiles . . . 196
Configuring E-mail Servers . . . 200
Configuring SNMP Nodes . . . 202
Using Component Information . . . 206
Exporting and Importing Configuration Information . . . 206
Exporting and Clearing Component Logs . . . 208

Performing System Maintenance . . . 213

Performing Routine Maintenance . . . 214
Performing Hardware Maintenance . . . 214
Performing Software Maintenance . . . 221
Troubleshooting . . . 233
Troubleshooting Hardware Issues . . . 233
Troubleshooting Software Issues . . . 236

Appendices . . . 241

Compatible Voice Cards . . . 242
Alarms Summary . . . 244
Using the Diagnostics Tools . . . 257
Correcting Checksum Mismatches . . . 259
Correcting Tampering . . . 259
Correcting Tampering from a Command Line . . . 261
Configuring Integration Service CTI Adapters . . . 262

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Alcatel Omni PCX 4400 via TSAPI 263
Aspect Event Bridge 265
Concerto for Aspect Unison/Ensemble/Ensemble Pro 267
Aspect Contact Server (Portal) 269
Avaya Definity G3/S8x00 via TSAPI 271
Avaya DLG Adapter 273
Avaya PDS 12 and 3.0 275
Avaya ASAI via CVLAN Adapter 277
BT Integration 279
Cisco CallManager with JTAPI 282
Cisco Call Manager 284
Genesys Adapter 286
Nortel Meridian/Succession via CTConnect 288
Nortel Meridian/Succession via MLS 290
ICM Adapter 292
eQuality Connect 294
Exec Record and TCP/IP API/Unify 296

Glossary **299**

Index **303**

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

About This Guide

The About This Guide section provides you with details about the guide's audience, a summary of each chapter, navigation aids, and where to find additional resources and help.

This introductory section to the guide describes the following topics:

- Intended Audience for This Guide, page 8
- Summary of Information Included in This Guide, page 9
- Related Documents, page 12
- Conventions Used in This Guide, page 13
- If You Need Help, page 15
- Contacting Technical Support, page 16

Intended Audience for This Guide

This document is intended to be used by system administrators involved with the configuration, management, and maintenance of the Full-time Recorder. It is intended to be used also by enterprise administrators and system integrators who set up a recording system for an organization.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Summary of Information Included in This Guide

This guide provides the following information:

Chapter title	Description
Chapter 1: Getting Started, page 19	Describes how to log in and how to create users.
Chapter 2: Working with Components, page 37	Describes Recorder components and how to configure them.
Chapter 3: Using Voice Cards, NICs and Analyzer, page 109	Shows how to configure voice cards and network interface cards.
Chapter 4: Managing System Components, page 183	Describes Recorder alarms and how to configure them and how to use component information.
Chapter 5: Performing System Maintenance, page 213	Describes routine hardware and software maintenance tasks.
Appendices, page 241	Lists compatible voice cards, alarms summary, encryption guidelines, how to correct checksum mismatches, and how to configure common Integration Service CTI adapters.
Glossary	Defines the terms you need to understand the Recorder.
Index	Lists topics that you can use to access information in the guide quickly.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

If your server has one or more roles other than Recorder, you may refer to information on specific areas, as shown in the following table:

Server Role	Refer to these sections:
Centralized Archiving	• Managing Archive Drives on page 66 • Configuring Centralized Archiving on page 106 • Monitoring Components with Alarms on page 184 • Alarms Summary on page 244 • Correcting Checksum Mismatches on page 259 See also the *Centralized Archiving Installation and Administration Guide.*
Screen Recorder	• Configuring Live Monitor and Observer on page 94 • Monitoring Components with Alarms on page 184 • Alarms Summary on page 244 See also the *Full-time Recorder Enterprise Manager Administration Guide*
Integration Service	• Configuring Adapter Settings on page 38 • Monitoring Components with Alarms on page 184 • Alarms Summary on page 244 • Configuring Integration Service CTI Adapters on page 262 See also the *Full-time Recorder Enterprise Manager Administration Guide* and the *Integration Service Guide*.
Analyzer	• Configuring Analyzer on page 170 • Alarms Summary on page 244

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

The following tabs appear in Recorder Manager (RM) when the indicated server role is installed on its own. The Screen Recorder role is not shown as it is the same as the respective TDM or IP Recorder.

	SERVER ROLE				
Recorder Manager Tab	**TMD Recorder***	**IP Recorder**	**IP Analyzer**	**Integration Service**	**Centralized Archiving**
General Recorder Settings	✓	✓	✓	✓	✓
Archive	✓	✓			✓
Voice Cards	✓	✓**			✓
Alarm Notification Profiles	✓	✓	✓	✓	✓
License	✓	✓			
Disk Manager	✓	✓	✓	✓	✓
Consolidator / Database Settings	✓	✓			✓
Import/Export	✓	✓	✓		✓
IP Extensions		✓			
Component Logs	✓	✓	✓		✓
Network Settings	✓**	✓	✓		
Compression	✓	✓			
Start/Stop Component Services	✓	✓	✓	✓	✓
Call Control			✓		
Alarms	✓	✓	✓	✓	✓
Live Monitor	✓	✓			
Recorder Status	✓	✓	✓	✓	
SNMP	✓	✓	✓	✓	✓
Integration Service				✓	
Manage User	✓	✓	✓	✓	✓
View RM Logs	✓	✓	✓	✓	✓
Email Server	✓	✓	✓	✓	✓
* Also known as ITS IP Recorder. ** Applies only for ITS Link switch IP emulation					

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Related Documents

The following documents are referenced in this document.

- *Full-time Recorder Enterprise Manager Administration Guide*
- *Enterprise Security Administration Guide*
- *Centralized Archiving Installation and Administration Guide*

The following documents are related to this document:

- *Full-time Recorder Installation Guide*
- *Full-time Recorder System Infrastructure Guide*
- *Integration Service Guide*
- *Viewer User Guide*

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Conventions Used in This Guide

The following two tables describe some of the conventions that are used in this document:

- The Standard Conventions table highlights conventions used to describe user interaction, as well as special notations
- The Information Icons table describes the icons used to highlight information of special interest to the user

Standard Conventions

Area	Description
Menu Items	Menu items are highlighted in bold as in the following example: From the menu, choose **File > Preferences > Options**.
Document Names	Other Verint Systems documents are referred to using italics. For example: Refer to the *Quality Monitoring 7.7 Installation Guide* for more information.
Buttons, Functions, and Dialog Box and Window Names	Specific button or function names are highlighted in bold. The following example shows how a button and dialog name are referred to in the documentation: Click **OK**, and then choose the **Restore Database** dialog box.
User Variables	When the user is expected to type a value, the name of the variable to be replaced is surrounded by < > . The following are examples: **<Your ER Server Name>** The notation **<Your ER Server Name>** refers to the name of your Enterprise Reporting server. When you see this notation, replace it with the actual name of your Enterprise Reporting server.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Information Icons

Icon Type	Function
Note	Important details that we want to make sure that you do not overlook.
Tip	Helpful hints that can improve the efficiency or effectiveness of your work.
Caution	Advice that can help you avoid undesirable results.
Warning	Situations that can result in: • Harm to software • Loss of data • An interruption in service

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

If You Need Help

Our goal at Verint Systems is to provide you with the best products backed by a high quality support network with a variety of resource options. These include:

- Verint Systems website and Customer Interaction Center (CIC)
- Telephone
- E-mail
- Direct Internet FTP
- Other support and training alternatives

Before You Contact Technical Support

Help from Technical Support is as near as your keyboard or telephone. However, before you contact us, read this section carefully. We can provide faster and better service if you have certain information available when you contact us.

You can solve many problems quickly with the information in the online Help system or in this manual. When running the product, you can select the **Help** button in the upper-right portion of the window to get help for the active window or dialog box.

If you are unable to solve a problem by using the online Help or this manual, and you need help from Technical Support, use the guidelines in the following checklist before you contact us:

1. Write down the problem and details that may help us solve the problem. If you can consistently reproduce the problem, list the steps to reproduce it.
2. Have at least the following information available when you contact Technical Support.
   - Your name and customer site number, and identify yourself as a customer, Verint Systems partner, or Verint Systems employee. Customer-initiated CIC contact is restricted to customers that are one of the designated support contacts on your company's service level agreement.
   - Product name and version number.
   - Server and client operating systems and service pack version numbers
   - Supporting files and screenshots (if available)
   - ACD type and reporting package (for ACD-related issues)
   - The wording of any error messages from the product and/or operating system
   - Has this problem occurred previously? If it is new, did you change your system configuration recently?

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Contacting Technical Support

Once you have determined that you need technical support, and you have gathered as much information as you can based on the checklist, the following provides a list of the various support options and alternatives:

Verint Witness Actionable Solutions Website and the Customer Interaction Center (CIC)

This facility allows users worldwide fast access to product information, marketing and sales information, information about the company, technical documentation, support case management, and support solutions information.

You can access the VerintWitness Actionable Solutions Customer Interaction Center (CIC) support site at www.witness.com/support, or through www.witness.com by clicking the **Support Login** link from the Home page.

Once you have successfully logged on to the CIC, use the navigation tree on the right to access available user manuals, troubleshooting guides, FAQs, and more.

For help using the site, refer to the *CIC Support Website Navigation Guide*. To access this document, click the link at the right on the CIC Home page. The guide is a PDF file that you can save or print locally for future reference.

Telephone

Verint Systems' Customer Interaction Center (CIC) provides the self-service tools and information you need to get the most out of your investment.

Americas:
+1 800 4 WITNESS (USA toll-free)
+1 770 754 1870

Europe/Middle East/Africa:
+0800 496 1111
+44 (0)1372 869 570

Hong Kong/Asia Pacific:
+852 8103 0104

Australia:
1 800 600 806

New Zealand:
+61 2 8223 9493

Japan:
+81 (0)3 5919 1875

For geographic locations and hours of operation, refer to www.witness.com\support\ and click on **Contact Centers**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Email

If you are a new customer and need a logon ID and password, you can e-mail support@witness.com to obtain your new logon information.

Direct internet FTP

This facility greatly speeds up transfer of new and upgraded software to all Witness Systems customers. Contact us for more information about access to Direct Internet FTP services.

Other support and training alternatives

In addition to documentation, online Help, and support services, Witness Systems also offers both classroom-based and online learning alternatives to suit your specific needs. Contact us for more information about other support and training alternatives.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Chapter 1

Getting Started

Getting Started describes the processes of logging in and setting up users on the local Recorder. Getting started is described in the following topic:

- Setting Up

For information on setting up the enterprise using Enterprise Manager, refer to the *Enterprise Manager Administration Guide*.

Setting Up

Setting Up describes logging into the system and creating authorized users. This is described in the following topics:

- Logging Into the System
- Configuring the Recorder License
- Creating Users
- Using System Logs
- Using Help

Logging Into the System

Logging in describes procedures for logging into the Recorder Manager and setting user preferences. Procedures are the same for first time login and your every day login. The only change is if you are a designated User Administrator, in which case you can add users and change passwords. Information is presented in the following topics:

- Logging in
- Setting User Preferences

If you access the Recorder Manager from Enterprise Manager, you do not need to type username and password again. Using Enterprise Manager, if available, to manage individual Recorders is advisable.

Logging in

Log in to authenticate yourself as a valid and registered user of the system. You must type the user name and password assigned by your system administrator.

To log in:

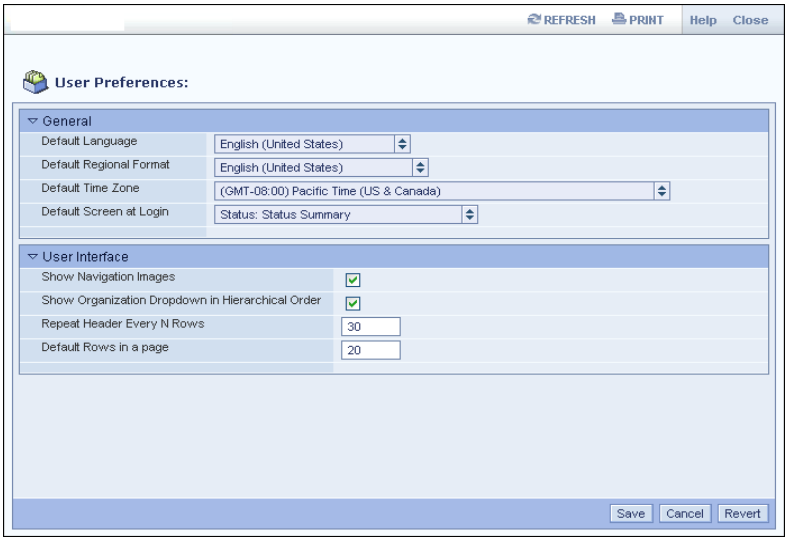
1. Optionally select a language from the dropdown list, if available. If no languages except English are available, you will not see an option to select a language.
2. Log in by clicking the desktop shortcut or by entering the url of the system such as **`http://recordername:PortNumber/RM`** (where recordername is the Recorder's server name and PortNumber is the server port number chosen at installation). For example, a login url could be **`http://10.1.4.169:8080/RM`**.
3. Type your login name.
4. Type the password provided. For first-time login, refer to the *Recorder Installation Guide.*
5. Click **Login**.

Note that the password can be changed after login by any authorized individual or User Administrator. To do this, click the **System** tab and then the **Manage Users** tab, select the login name, and then select **Change Password**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Setting User Preferences

Set system preferences to establish the global settings for Recorder Manager. The fields presented in this screen result from the preferences established within the Workforce Optimization application.



To complete the General area:

Complete the General Preferences area to choose language and time preferences by doing this:

1. For **Default Language** (where available) choose a language. Default is English (US).
2. For **Default Regional Format** choose a regional time format, such as English, 24 Hour.
3. For **Default Time Zone** choose your time zone. Default is Pacific Time (US & Canada)
4. For **Default Screen at Login** choose the first screen to be displayed after you log in

To complete the User Interface area:

Complete the User Interface area by following these steps:

1. For **Show Navigation Images,** check to show or hide the iconic images above the tab names in the navigation bar.
2. For **Show Organization Dropdown in Hierarchical Order**, check to show all organizations in the Organization dropdown in a tree (hierarchical) structure. When unchecked, only organizations in the user's scope display.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 For **Repeat Header Every N Rows,** type a number that indicates how the number of rows before your header repeats. For example, choose 25 and the header will appear every 25th row.

4 For **Default Rows on a Page,** type the number of rows shown in a page, such as 25. Then 25 rows will show in each page. Recorder Manager uses pagination (that is, a separate page) to show the data in multiple pages.

Caution: Do not select a large number of records in a page. Scrolling through many records on a page can cause usability issues.

5 Click **Save** to save your changes

Notes:

- User Preferences apply to all users of the Recorder Manager. System defaults are set by the Administrator.
- If you make a preference change in What If mode, that change affects Production mode, and vice versa.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring the Recorder License

Recorder licensing is designed to provide the maximum amount of flexibility in terms of license coverage. You can have one of the following license types:

- **Temporary**. This is a 10-day trial license that licenses up to a maximum of 400 concurrent recordings. Recordings during this time are maintained, that is, kept on file, when you upgrade to a full license.
- **Full.** This is a license for a specified number of concurrent contacts that can be recorded.

The licensing key includes options to enable or disable audio and screen channels (Enable Audio and Enable Screen). The **Number Of Channels** field is a common field in the license key for both audio and screen channels. It gives the total number of concurrent licensed recordings for Audio if enabled (Enable Audio is selected) and the total number of concurrent licensed recordings for Screen if enabled (Enable Screen is selected).

Each Capture Engine (audio or screen) has its own pool of Channels, so that if a particular Capture Engine runs out of licensed channels then it cannot use a licensed channel from the other Capture Engine. For example, if both Audio and Screen are Enabled and **Number Of Channels** is set to 200 then 200 licensed concurrent Audio recordings and 200 licensed concurrent Screen Recordings are allowed. If an Audio Capture engine processes 200 concurrent recordings and the Screen Capture Engine processes 99 concurrent recordings then if a new start record request comes to Audio Capture Engine to record on a new channel then Audio Capture Engine returns an error message and raises an alarm indicating it exceeded the licensed concurrent channels limit as it is already processing the 200 concurrent recordings. In effect, the Audio Capture Engine cannot use a channel from the Screen Capture Engine channel pool, where some licensed channels are idle.

The type of license depends on the license key provided to you. This information shows in the license window after your license application has been processed. License information also shows in terms of a *soft* license in the Recorder's status summary page.

More information on *soft* licensing:

A *soft* license (a software-based limit equal to licensed concurrent contacts that can be recorded minus 10) is built into every recording license. The *soft* license is used to trigger alarms as the license limit is approached. The *soft* license also ensures that you are warned well in advance before the license limit is reached. When the license limit is reached, no contacts are recorded until the number of concurrent calls falls below the license limit.

License statistics appear in the Recorder's Status Summary which is accessed from Recorder Manager (**Status > Status Summary**). These statistics keep you informed about the number of contacts in progress, contacts within the *soft* license limit, and contacts that exceeded the *soft* limit. Contacts that exceed the *soft* limit are shown as unlicensed contacts.

Recorder alarms are triggered when the *soft* license limit is approached. For example, if you purchase a license for 100 concurrent recordings, then your soft limit is set at 90. When the recorder reaches 91 concurrent recordings, the *License Reaching Max Limit*

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

alarm is triggered. This alarm warns you that you are approaching the real license limit (but have not yet exceeded it). When contact recording number 101 appears, the Recorder does not record it, and the alarm *License Max Limit Reached* is triggered.

There are times when the *soft* limit may be of no value. If you have a TDM Recorder, you may have purchased a concurrent recording license equal to your number of channels. In this case, the alarms mentioned above may be less interesting to you because you would never have to worry about having more contact recordings than you can record, because this is not possible. If the alarm is of no value, you could go into the Alarm configuration in Recorder Manager and disable the *License Reaching Max Limit* alarm so that you do not get a warning message or e-mail every time the call center has a busy day.

Activating the Recorder License for the First Time

When you login in to the Recorder when installing the system, you are required to confirm your license or apply for a temporary one. The first time you log in to the newly-installed application, you use the provided user ID and password. You then must change the password and use the new password every time you access the application.

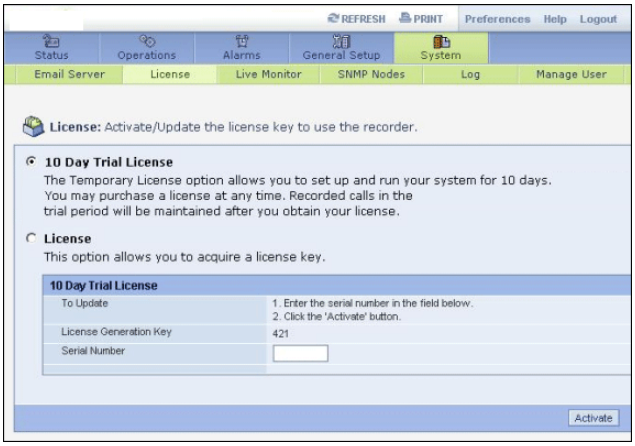
A license is bound to the MAC address of a network interface card on the recorder. If the network interface card to which the license is bound becomes inactive, the license is invalidated. This is true when the card is disabled, physically removed, or unconfigured with TCP/IP. Users must therefore unconfigure the Internet Protocol (TCP/IP) using Recorder Manager before activating the recorder license. Configuring and unconfiguring NICs is described in *Setting up Network Interface Cards* in the *System Administration Guide*.

To activate the Recorder license for the first time:

1. Launch the Recorder Manager and choose a language.
2. Enter the username and password supplied and click **Activate**.
3. At any time while using Recorder Manager you can access the license screen by choosing **System > License**.

   NOTE: The 10-Day trial license and permanent license radio button options appear only at the first time a recorder's license is configured. After that, only the License option is available.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



4 In the Site License window do one of the following, and then click OK:

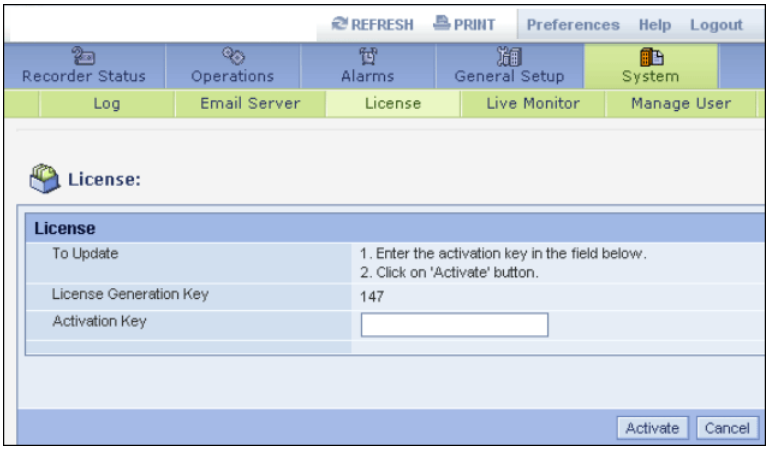
- To install a temporary, 10-day license, click **10-Day Trial License**.
- To install a permanent license, select **License**.

A different window displays according to your selection.

5 If you choose the **10-Day Trial License** option, enter the serial number supplied or enter a pre-determined 6-digit serial number in the range 600000 - 699999. This license is good for recording up to 400 concurrent contacts, which are maintained if you choose to upgrade to a full license. Finish by clicking **Update** in the license summary screen that displays.

6 If you chose the **License** option, follow screen instructions, and then type in an Activation key for your full license.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



7 Click **Activate**.

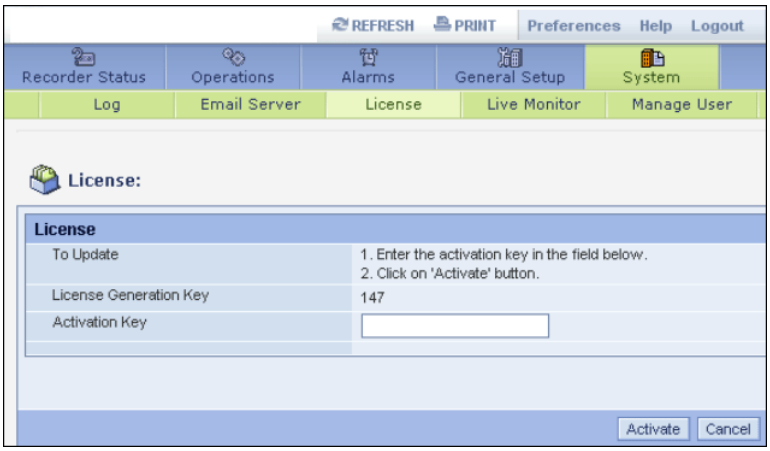
Re-activating a Recorder license

Use the re-activate license method for updating your software license to activate a full license based on a temporary one, or when upgrading the features in your license, such as adding more channels or adding screen recording.

To re-activate a Recorder license:

1 In Recorder Manager click **System > License**. The License screen displays.

2 Copy the Activation Key field, and then click **Update**.



3 In the **Activation Key** area, type in the activation key.

4 Click **Activate**.

NOTE: If the license has an Expiration date, a warning message displays during the final 10 days.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Creating Users

Add or delete users of the Recorder to authorize access with full privileges by designated individuals. You can also assign and change passwords. You need to have a login with **User Administrator** privilege to create other users. The Superuser login by default has this privilege. If a user does not have User Administrator privileges, they can see only their own name and can only change their own password.

This information is described in the following topics:

- Viewing Authorized Users
- Adding Users
- Editing Users
- Changing a Password
- Deleting a User

Viewing Authorized Users

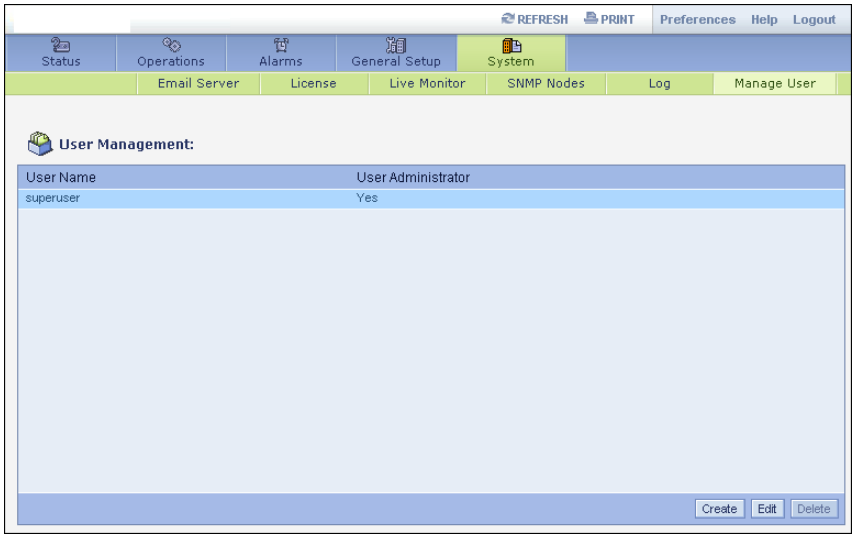
View existing authorized users to access a current list of persons who are authorized to use the Recorder Manager. After selecting a user, you can perform add, edit, delete and reset password tasks.

To view authorized Recorder users:

1 Click **System > Manage User**.

The User Management screen displays listing users already created. The system comes with a pre-defined super-user login, as described in the *Recorder Installation Guide*. This login name can be deleted only by another user with User Administration privileges.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Do one of the following:

- Click **Create,** and then create users as described in Adding Users on page 28.
- Select a username, and then click **Edit** or **Delete**.
- To change a password, select a username, and then click **Edit**.

It is recommended that you change the default superuser password after logging in for the first time, as described in Adding Users on page 28.

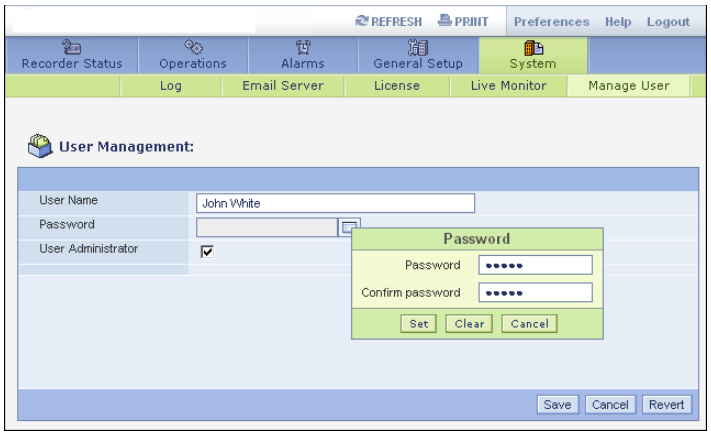
Adding Users

Add users to provide authorized individuals with a user name and password that will allow them to log into the Recorder. By default, users have unrestricted access to all features. Users added in this screen can be marked as a User Administrator if the User Administrator checkbox is checked. This means that the users created in this way can create and manage other users.

To add a user:

1 Click **System > Manage User,** and then click **Create**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Complete the User fields as follows:

Field	Description
User Name	Type the username of the user, such as *admin* or *jsmith*.
Password	Click the folder icon to show the Password screen then type a password. The password should be secure and not easy to guess. Password fields are case sensitive.
User Administrator	Check to indicate that this user has the status of **User Administrator.** With this status, users have permission to add, edit and delete other users, change passwords, and grant or decline the status of User Administrator. If this checkbox is unchecked, the indicated person does not have privileges to add other users. When they log in, they see only their own names and not other authorized users.

3 Click **Save.**

Editing Users

Use the Edit function to edit usernames and change passwords.

To edit a user:

1 Click **System > Manage User** and select a user.

2 Click **Edit**.

3 Complete the password field as described in Changing a Password on page 30.

4 Click **Save**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Changing a Password

Reset a password to assign a new password or replace a forgotten or lost password. User Administrators can change passwords for anyone. Users who are not designated as User Administrors can only reset their own password.

To change a password:

1. Click **System > Manage User**.
2. Select the username of the password to be reset, and then click **Edit**.
3. Click the folder icon beside Password.
4. In the Password window, type the new password, confirm by re-entering, and then click **Set**.
5. Note the password for distribution to the user.
6. Click **Save**.

Deleting a User

Users with the role of User Administrator can delete any user from the list, including the Superuser. You cannot delete your own name.

To delete a user:

1. Click **System > Manage User**.
2. Select the user (except yourself) to be deleted and click **Delete**.
3. Click **Yes** to confirm the deletion.

Using System Logs

Use system logs to manage configuration files, view logs and view audit trails. Ths information is presented in the following topics:

- System Log Manager
- System Log Viewer Configuration
- Viewing Log Files
- Customizing the Log Viewer Display

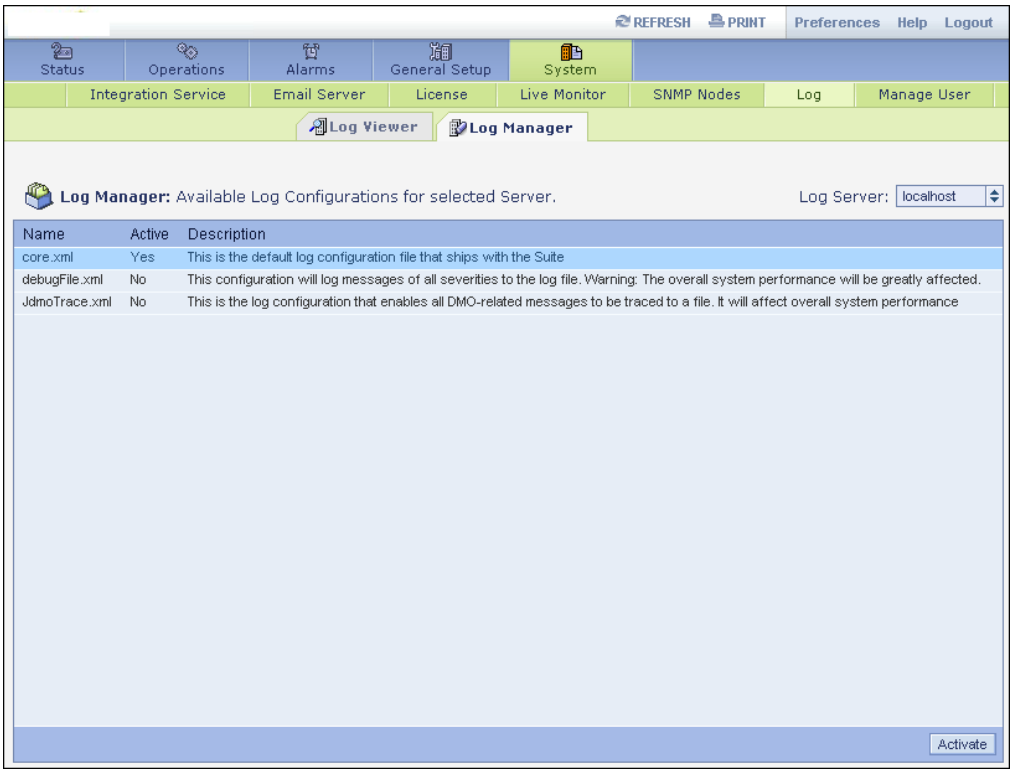
System Log Manager

Use the Log Manager to access log file configuration options. This allows you to enable or disable the generation of selected log files. Log configurations are created and stored as XML files.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To set the log configuration:

1 Click **System > Log > Log Manager**. The Log Manager window displays.



2 Review fields according to the following:

Item	Description
Log Server (dropdown menu)	Shows the server(s) in which the log files are being configured. For example, shows **Localhost** if you accessed Log Manager from a local Recorder Manager, or shows a list of selectable Recorder servers, if you accessed Log Manager from Enterprise Manager.
Name	Shows the name of the log file.
Active	Toggles between **Yes** and **No**, which are options that enable or disable the generation of logs for the named file.
Descriptions	Shows a description of each named file.

3 Highlight the log configuration file and click **Activate**.

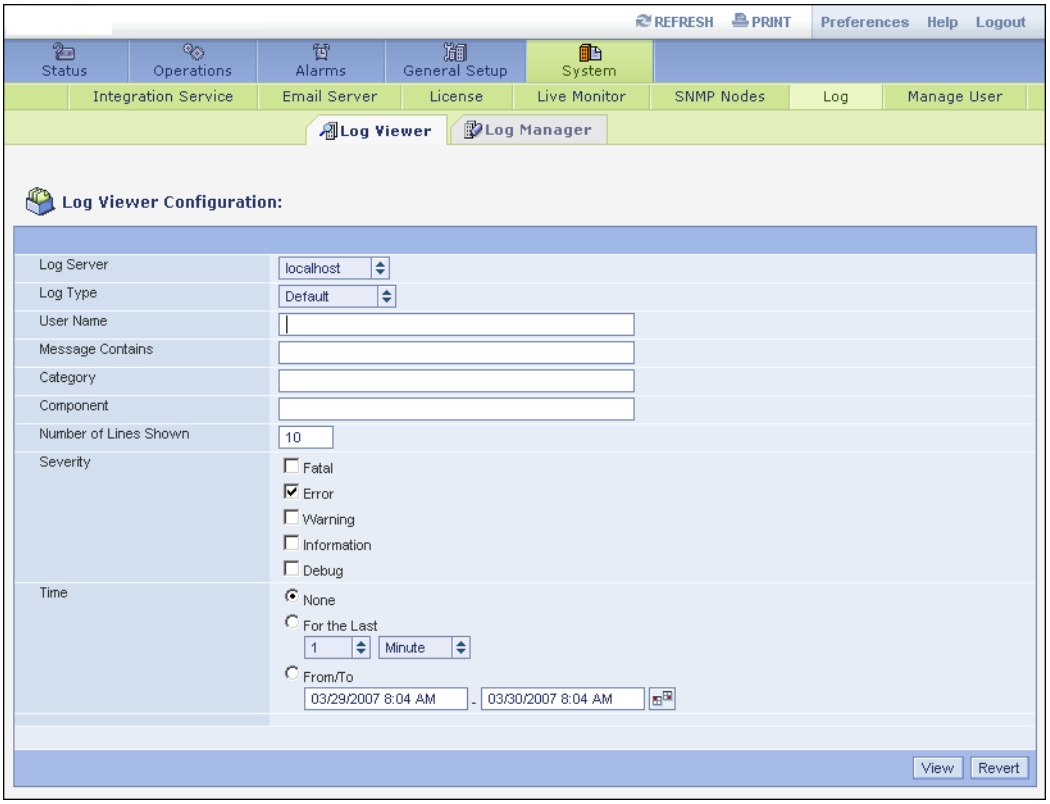
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

System Log Viewer Configuration

Use this page to configure and view your System Log. These settings filter the information displayed in the Log. The application records all actions that will result in a modification or change to the configuration. An administrator accessing a configuration is not logged. The application also logs all error and warning conditions that occur within the Recorder Manager application.

To configure the Log Viewer:

1 Click **System > Log > Log Viewer**. The Log Viewer window displays.



2 Select the log server from the list. If you accessed Log Viewer from a local Recorder Manager, **Localhost** displays, or if you accessed Log Viewer from Enterprise Manager, a list of selectable Recorder servers displays.

3 Select the type of log from the list.

4 Type the user name to filter by. Leave the field blank to display data for all users.

5 Type message contents to filter by. Leave the field blank to display data for all message contents.

6 Type the category to filter by. Leave the field blank to display data for all message categories.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

The category is a specific Java class name that logged the error. For example:

`ejb.bpx.am.msgProcessor.MessageQueueConnector`

7 Type the component to filter by. Leave the field blank to display data for all message components.

The component is the package or area of the application that contain the class that logged the error. For example:

`web.bbm, bpfx, ejb.am`

8 Type the number of lines to be displayed at one time.

9 Check the severities of the errors you want displayed. Choices include Fatal, Error, Warning, Information, and Debug,

10 Select the time period to be displayed. Select **None** to display events for all time periods covered by the log, or select a time range.

The next time the user logs in or views this page, the settings that were used last will be automatically populated.

11 Click **View** to view logs with the displayed settings, as described in Viewing Log Files on page 33.

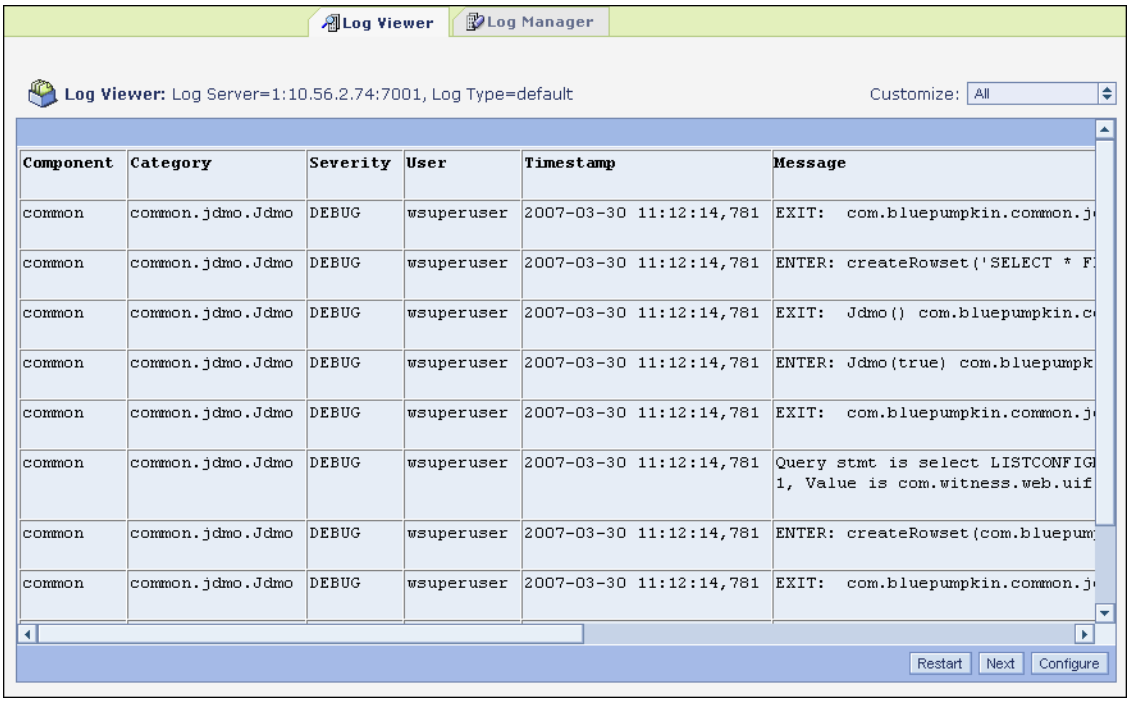
Viewing Log Files

View log files to obtain detailed information on the logs you configured in Log Viewer, typically for troubleshooting and diagnostic purposes. For example, if you set the severity level to show only errors, then you can view only messages with a severity level of Error. You can also customize the display of log file information to show all or only selected categories.

To view log files:

1 Perform all the steps as described in System Log Viewer Configuration on page 32. After you click **View**, the Log Viewer window displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.


Log Viewer
Log Manager
Log Viewer: Log Server=1:10.56.2.74:7001, Log Type=default
Customize: All
Component Category Severity User Timestamp Message
common common.jdmo.Jdmo DEBUG wsuperuser 2007-03-30 11:12:14,781 EXIT: com.bluepumpkin.common.j
common common.jdmo.Jdmo DEBUG wsuperuser 2007-03-30 11:12:14,781 ENTER: createRowset('SELECT * F
common common.jdmo.Jdmo DEBUG wsuperuser 2007-03-30 11:12:14,781 EXIT: Jdmo() com.bluepumpkin.c
common common.jdmo.Jdmo DEBUG wsuperuser 2007-03-30 11:12:14,781 ENTER: Jdmo(true) com.bluepumpk
common common.jdmo.Jdmo DEBUG wsuperuser 2007-03-30 11:12:14,781 EXIT: com.bluepumpkin.common.j
common common.jdmo.Jdmo DEBUG wsuperuser 2007-03-30 11:12:14,781 Query stmt is select LISTCONFIG
1, Value is com.witness.web.uif
common common.jdmo.Jdmo DEBUG wsuperuser 2007-03-30 11:12:14,781 ENTER: createRowset(com.bluepum
common common.jdmo.Jdmo DEBUG wsuperuser 2007-03-30 11:12:14,781 EXIT: com.bluepumpkin.common.j
Restart
Next
Configure

Review information in the Log Viewer window according to System Log Viewer Configuration on page 32.

2 Do one of the following:

- Click **Restart** to return to the beginning of the page.
- Click **Next** to review the next batch of messages on the page, (instead of using the scroll bar to view the additional messages).
- Click **Configure** to return to the Log Viewer window, as described in System Log Viewer Configuration on page 32.
- Select **Edit** in the **Customize** menu (at the top of the window), and follow procedures described in Customizing the Log Viewer Display on page 34..

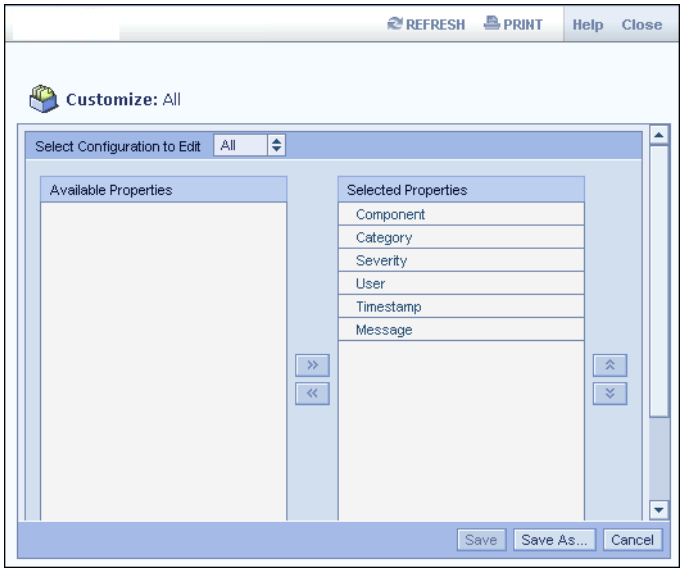
Customizing the Log Viewer Display

Customize the display of log messages to choose log file properties to display or to rearrange the display of properties (that is, columns) such as the time stamp in the Log Viewer report.

To customize the log viewer display:

1 Follow procedures as described in Viewing Log Files on page 33 and click **Edit** in the Customize dropdown menu (at the top of the window). The Customize window displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Complete the Customize window by clicking the left/right arrows to move Available and Selected Properties, or by clicking the up/down arrows to rearrange the sequence in which the log file properties display in the log viewer.

3 Click **Save** to save the default customization, or click **Save As** to save as a different name that will appear as a menu item in the Customize drop down.

Using Help

You can access help through online help or by referring to this guide. To obtain information about the current screen in Recorder Manager, click the Help button. Information in online help is identical to information in the *System Administration Guide* (this guide). You can display the Table of Contents in online Help. Use the Index function to search the index. Use Search to locate topics containing key words that you enter

You can also print this guide to reference the procedures. To print, locate the PDF file for this guide on your network. Next, open the PDF, and then click Print. You may have to ask other users for the location of the PDF files. Once printed, use the guide's TOC or Index to retrieve information.

To view help topics:

1 In any window, click **Help**. The help topic for that window displays.

2 Click the secondary heading in the window to show the help contents.

3 Click the heading again to hide the help contents.

Popup blockers must be switched off in Internet Explorer to view help properly.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To view related topics:

1. In any window, click **Help**. The help topic for that window displays.
2. Click the **Related Topics** icon at the bottom of each topic window. This icon also appear in the upper right side of the menu bar.
3. Click a topic in the **Related Topics** window to launch help on that topic.

To use the help table of contents:

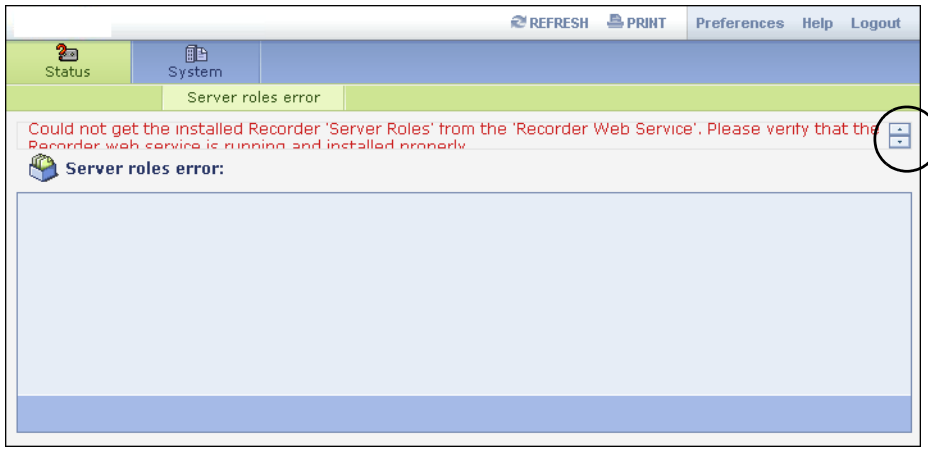
1. In any window, click **Help**. The help topic for that window displays.
2. Click the bookmark symbol beside the navigation arrows in the menu bar. The table of contents displays.
3. Click the plus (+) symbol beside topics to expand and view subtopics. Click the minus (-) symbol to hide subtopics.
4. Click **Index** to view an alphabetical list of indexed topics.
5. Click **Search** and type search words to search for topics containing key words.
6. Click **Refresh** to hide the table of contents.

To cycle through help topics:

1. In any window, click **Help**. The help topic for that window displays.
2. Click the navigation arrows (up and down triangles) in the menu bar to cycle through all help topics.

Using System Messages

You can get immediate help by viewing system messages that appear on most windows. Sometimes you need to click the scroll arrows to read longer messages.



Click the scroll arrows to view longer system help messages

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Chapter 2

Working with Components

Working with Components describes how to configure, manage, and monitor each of the Recorder's system components, excluding voice cards, and NICs, using the Recorder Manager. To perform any of these tasks you must be authorized to access all features. Information is presented in the following topics:

- Configuring Integration Service CTI Adapters
- Configuring Common Components
- Configuring IP Recording Components
- Configuring Optional Components

Configuring Integration Service CTI Adapters

Configure your Integration Service CTI adapter to set up the connection between the Data Source (your switch or PBX) and your Recorders. By configuring your adapter in Recorder Manager (RM), you are creating a link to a CTI Server and associating it to a Data Source configured within Enterprise Manager (EM). You are also configuring what custom attributes from the CTI Server the Adapter should pick up and make available to the rest of the system. You must set up the Integration Service in EM before configuring CTI adapters, as described in the *Integration Service Guide*.

Configuration of the Integration Service CTI Adapter is only necessary if Integration Service is going to be used for tagging or recording control. If only Unify is being used with the Recorders then configuration of CTI Adapters is not necessary. Also the Integration Service tab within RM is accessible only if an instance of the Integration Service is installed on the Recorder that is running the RM.

For backward compatibility, Unify and the Integration Service can both exist in the same installation.

You configure adapters in three steps: you first select a CTI adapter, then apply to it the settings for your environment, and finally you optionally assign software attribute names (metadata) to be used by the Recorder. These tasks are described in the following topics:

- Configuring Adapter Settings
- Configuring Adapter Custom Attributes

Note: Graphics shown are for illustration purposes only and are subject to change.

Configuring Adapter Settings

Configure adapter settings to add, edit, and delete the settings that relate to your CTI adapter. This information is included in the following topics:

- Selecting your CTI Adapter
- Viewing CTI Adapter Details
- Creating and Editing Adapter Settings
- Deleting an Adapter
- Starting and Stopping Adapters

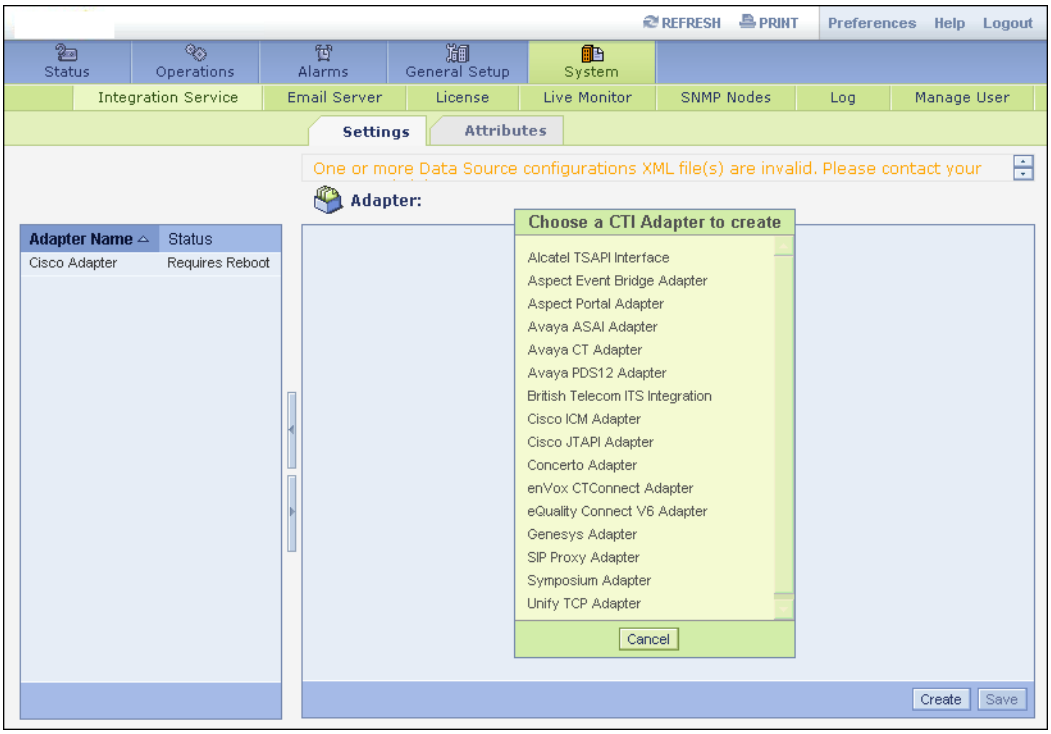
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Selecting your CTI Adapter

Select your CTI adapter to configure an adapter that is compatible with your switch. CTI adapters that you can create are listed in alphabetical order. After creating the adapter, it appears in the left pane along with its current status.

To select your CTI adapter:

1 Click **System > Integration Service** and then click **Create**.



Adapter names shown are for illustration purposes only and are subject to change.

2 Click the CTI Adapter you wish to use for integrating to the desired CTI server. You can find complete descriptions of each CTI Adapter type, the switch they are used for, and their available parameters, in Configuring Integration Service CTI Adapters on page 262.

Tip: A CTI Adapter is a component that connects to a CTI Server which relays events from a PBX, Dialer, or other Data Source, to the Integration Service subsystem. Typically, configuration of the CTI Server is the responsibility of either the customer or the switch vendor. The Integration Service CTI Adapter is configured by you.

3 Follow procedures in Creating and Editing Adapter Settings on page 41.

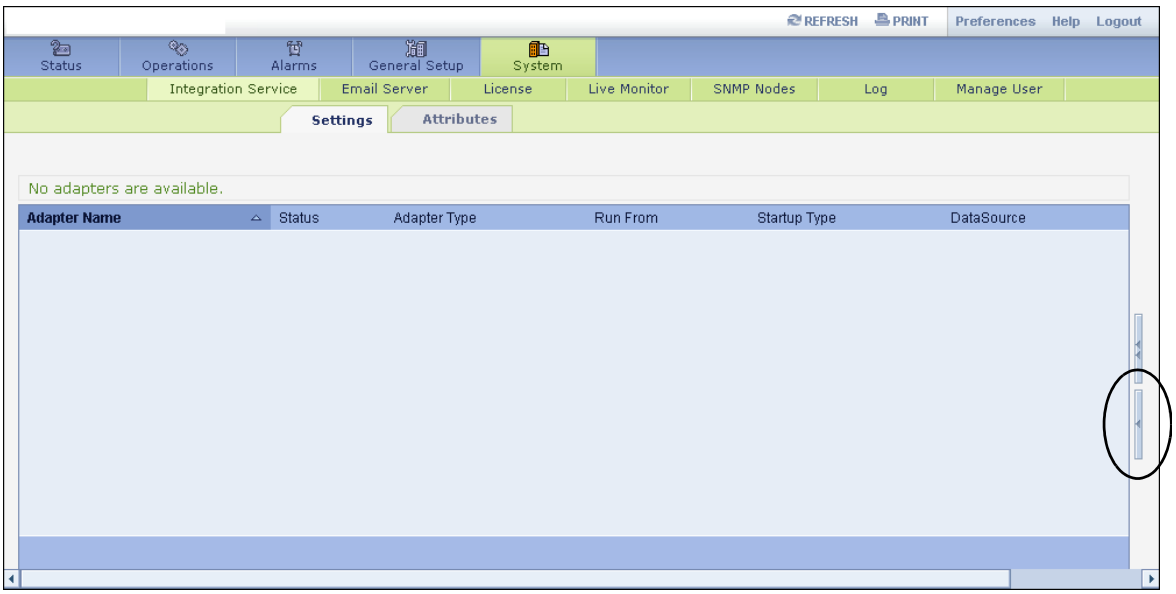
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Viewing CTI Adapter Details

View CTI adapter details to obtain additional information on the basic properties of CTI adapters. Properties include status, adapter type, startup type, and Data Source. Data Sources are configured in Enterprise Manager.

To view CTI adapters:

1 Click **System > Integration Service,** and then click the right-pointing arrow in the centre of the screen. The Adapter (left) pane displays full screen.



In the above illustration, no adapters are listed as none are currently available. Normally one or more adapters show here, providing Integration Service is used.

2 Review information according to the following:

Item	Description
Adapter Name	Shows the name of the CTI adapter.
Status	Shows the status of the Adapter. Choices include **Automatic, Manual,** and **Disabled**.
Adapter Type	Shows the type of the adapter, such as Genesys Aspect, or Alcatel.
Run From	Shows the component from which the adapter is run.
Startup Type	Shows the method in which the adapter is started. Choices include **Start, Stop** or **Restart**. Only the applicable options are enabled.
Data Source	Shows the type of the Data Source to which the adapter connects, such as Dialer, LAN, Phone, or Trader.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 Click the left-pointing arrow (circled) to return the screen to the original bi-pane display.

Creating and Editing Adapter Settings

Create or edit your CTI adapter to provide settings, such as a username or Data Source, for your Integration Service. Settings vary by adapter. These settings are then used to link your Data Source to the Integration Service of your recording system.

1 Follow the steps described in Selecting your CTI Adapter on page 39 to create a new adapter. To edit an adapter, select an existing adapter displayed in the left pane, and then type new information in the right pane and click **Save**.

2 Choose a CTI adapter compatible with your switch or server from the following list:

- Alcatel Omni PCX 4400 via TSAPI on page 263
- Aspect Event Bridge on page 265.
- Concerto for Aspect Unison/Ensemble/Ensemble Pro on page 267
- Aspect Contact Server (Portal) on page 269
- Avaya Definity G3/S8x00 via TSAPI on page 271
- Avaya DLG Adapter on page 273
- Avaya PDS 12 and 3.0 on page 275
- Avaya ASAI via CVLAN Adapter on page 277
- BT Integration on page 279
- Cisco CallManager with JTAPI on page 282
- Cisco Call Manager on page 284
- Genesys Adapter on page 286
- Nortel Meridian/Succession via CTConnect on page 288
- Nortel Meridian/Succession via MLS on page 290
- ICM Adapter on page 292
- eQuality Connect on page 294
- Exec Record and TCP/IP API/Unify on page 296.

3 Click **Save**. The new adapter displays in the left pane.

Deleting an Adapter

When an adapter is deleted a warning message displays, advising that the deletion process may take several minutes.

To delete a CTI Adapter:

1 Click **General Setup > Integration Service > Settings**. A list of all current adapters displays in the left pane.

2 Select an adapter in the left pane

3 Click **Delete**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Starting and Stopping Adapters

Start and stop adapters to control the ability of a selected CTI adapter to participate in the recording process by starting and stopping the connection between the PBX/switch and the Recorder. The displayed status of the adapter, either Automatic, Manual, or Disabled, determines the start and stop options.

To start and stop adapters:

1. Click **System > Integration Service > Settings**. A list of current adapters displays.
2. Select an adapter in the left pane. Details of that adapter show in the right pane.
3. Review the **Startup Type** field and then click **Start**, **Stop** or **Restart** as necessary. Only the applicable options are enabled. For example, if you need to restart, then only the **Restart** button is enabled.

Configuring Adapter Custom Attributes

Configure adapter custom attributes to provide attribute details, in what eventually turns out to be contact (call or screen) metadata, and associate custom attributes to an external name in Recorder Manager. This information is described in the following topics:

- Editing Adapter Custom Attributes
- Creating Custom Attributes in Enterprise Manager

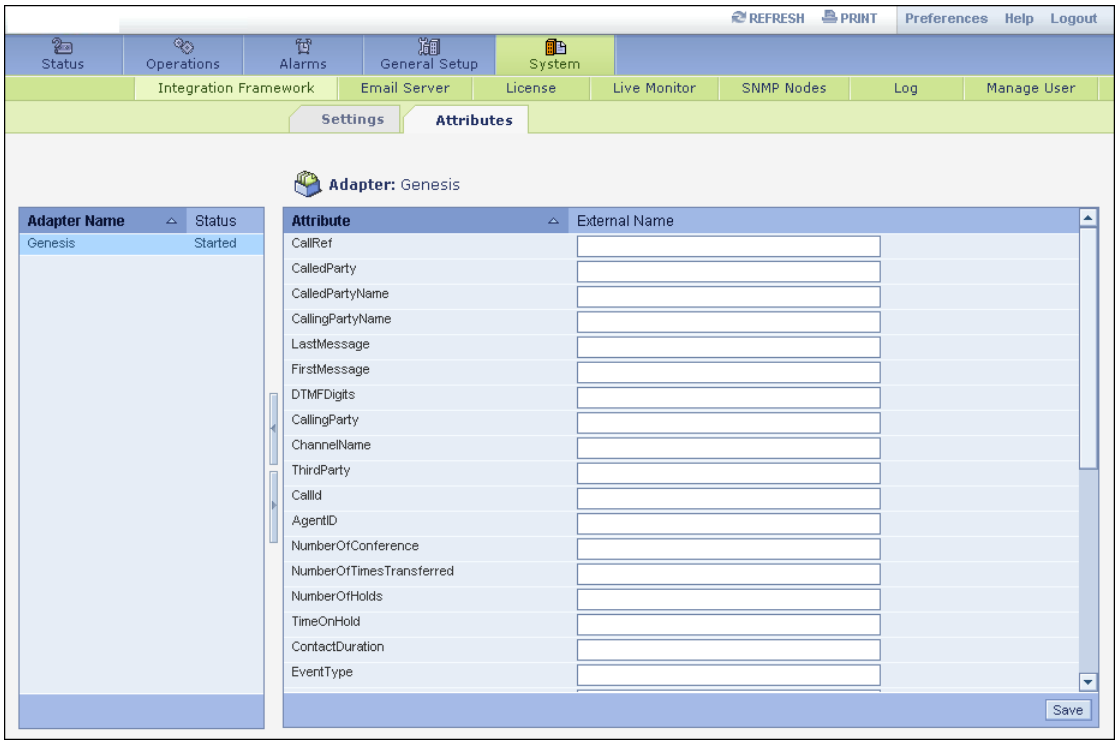
Editing Adapter Custom Attributes

Edit the custom attributes of an adapter to associate an external name in Recorder Manager. Custom attributes are created in Enterprise Manager and retrieved by Recorder Manager. The custom attribute's external name can be chosen from the available list of external names that are dynamically retrieved from the data store.

To edit an adapter's custom attributes:

1. Click **System > Integration Service > Custom Attributes**. A list of all current adapters displays in the left pane.
2. Select an adapter in the left pane. Any attributes for that adapter display in the right pane. The following illustration shows only a partial list of attributes.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



3 Choose an external name for custom attributes according to the following:

Attribute	Description
PauseDuration	The pause duration in seconds
CallRef	The reference number of the call
CalledParty	The identification of the called person in the case of a Cisco switch
CalledPartyName	The name or Agent ID of the called person in the case of a Cisco switch.
CallingPartyName	The name of the party that initiated the call.
LastMessage	The last message sent by the Recorder.
FirstMessage	The first message sent by the Recorder.
DTMFDigits	The ANI-related tones generated by a touch tone telephone to denote the 10 numbers, star, and pound keys on a telephone.
CallingParty	The identification of the party that initiated the call.
ChannelName	The name assigned to the channel (maximum 24 for T1, 30 for E1).
ThirdParty	Identification of a third party in the call.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Attribute	Description
CallId	The identification of the call in the switch queue.
AgentID	The logon ID of the agent
NumberOfConference	The total number of conference events in the contact.
NumberOfTimes Transferred	The total number of transfers in the contact.
NumberOfHolds	The total number of holds in the contact.
TimeOnHold	The total amount of time in seconds the contact was on hold.
ContactDuration	The contact duration in seconds.
EventType	Event in a call, such as Agent Level, System Level, CTI Level, Contact Level.
TrunkGroup	The Trunk Group on which the contact is being recorded.
Trunk	The Trunk on which the contact is being recorded.
NumberDialed	The number dialed.
DNIS	The Dialed Number Identification Service
CallDirection	Choice for the call direction.
CallType	Type of the call
ANI	The Automatic Number Identification or Caller ID.
DataSourceName	The name of the switch.
Queue	The switch queue.
Extension	The Agent's phone extension.
DeviceName	Either the Primary extension or workstation name.
SupervisorName	The supervisor of the agent involved in the call.
Attribute External Name	**Heading**
Skill	The skill of the Agent on the switch, such as Genesys skills.
LoggedOnDuration	The length of time the Agent was logged on the switch.
AgentName	The agent involved in the call.

All of the above attributes are available in the Attributes area in Enterprise Manager (EM). Any custom attributes created in EM appear as an attribute in the Recorder Manager Custom Attributes area of the Integration Service.

4 Click **Save**. The attributes are saved for the selected adapter.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Creating Custom Attributes in Enterprise Manager

If your organization has Enterprise Manager (EM) and you have the required security privileges, you can create custom attributes additional to those available by default to Recorder Manager.

To create additional Custom Attributes in EM:

1. In Enterprise Manager, click **System > Attributes > Settings**. The Create Attribute window displays.
2. Click **Custom** in the left pane and then click **Create** in the right pane.
3. Complete the fields in the Create Attribute window. Refer to EM online help for more information.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Common Components

Configuring common components describes how to configure Recorder components that are common to all environments. In all cases you use Recorder Manager to perform configuration tasks. You need to have the necessary security authorization.

Information is described in the following topics:

- Viewing the Recorder's Status
- Setting up the Recorder
- Configuring Archive
- Configuring Disk Manager
- Configuring Database Settings

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Viewing the Recorder's Status

You can view a Recorder's status based on component category and component details. The main status summary page provides a quick, visual update on basic Recorder components and how the Recorder is working. For more detailed information, you can view statistics on the Capture process and the Integration Service. All other statuses can be found under Other Status. The components displayed in the status depend on the Recorder components installed on the system. For example, if Integration Service is not installed, the Integration Service related status is not available.

Information is presented in the following topics:

- Viewing a Recorder's Status Summary
- Editing Status Summary Thresholds
- Viewing Capture Status
- Viewing Integration Service Status
- Viewing the Status of Other Components

Viewing a Recorder's Status Summary

View a Recorder's Status summary to obtain a quick, visual snapshot of the Recorder's current operational status. Use this function to monitor the overall health of the Recorder. Colorful smiley and frown symbols display to help you understand. Colours mean the following:

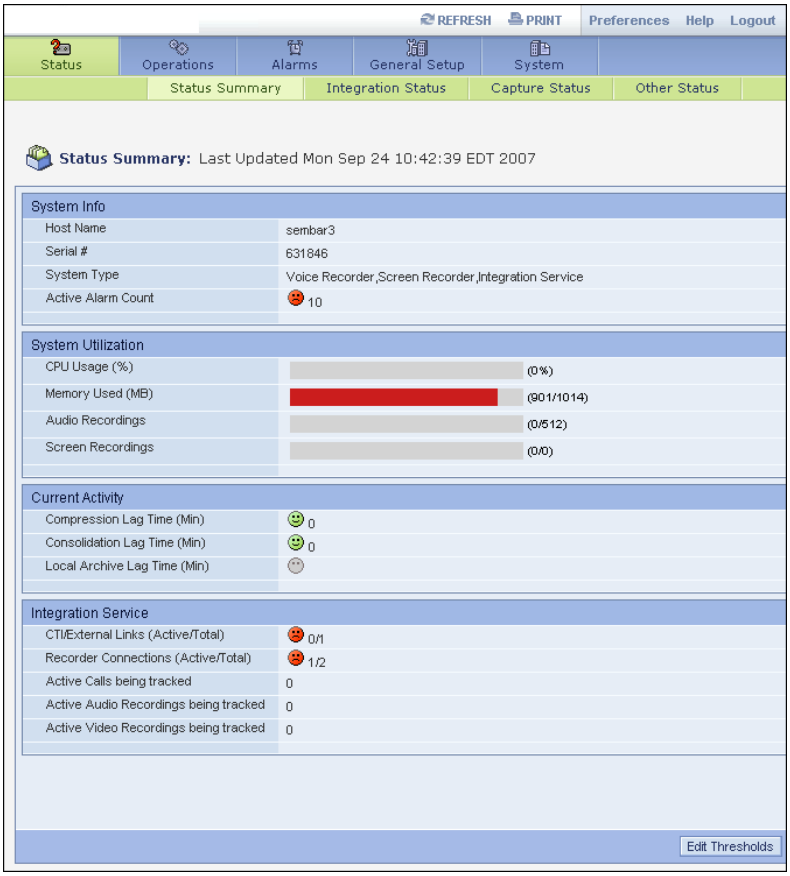
- Green Smiley: All is well.
- Grey Smiley: Unknown status.
- Orange Frown: Warning
- Red Frown:Error

To view a Recorder's status summary:

1 Launch Recorder Manager, and then click **Status.** The status summary window displays, showing a snapshot of Recorder performance activity.

Note:Different information displays according to the use of the Recorder. For example, a License tab does not display in a standalone Centralized Archiving server, as licensing is not required for Centralized Archiving.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Review status summary information according to the following:

Field	Description
System Info.	**Heading for information about the PC**
Host Name	The name of the PC.
Serial #	The serial number of the Voice or Screen Recorder. A serial number is not used with Analyzer.
System Type	The type of system, either one or more of a Voice or Screen Recorder, Integration Service server, Analyzer server, or Centralized Archive server.
Active Alarm Count	The number of currently active alarms.
System Utilization	**Heading for information about PC (System) performance. For Thresholds, refer to** Editing Status Summary Thresholds **on page 50.**

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
CPU Usage (%)	Shows the percentage of the central processing unit's cycles being used, including all related activities such as archiving and disk processing. High usage indicates high usage of the processor (CPU).
Memory Used (MB)	Shows the amount of memory (RAM) in megabytes currently being used by the PC.
Audio Recording	Shows the number of audio recordings currently in progress. For detailed capture settings, refer to Viewing Capture Status on page 52.
Screen Recording	Shows the number of screen recordings currently in progress. For detailed capture settings, refer to Viewing Capture Status on page 52.
Current Activity	**Heading for information on current PC activity. For Thresholds, refer to Editing Status Summary Thresholds on page 50.**
Compression Lag Time (Min)	Shows a graphical representation of the amount of time in minutes that the compressor component is behind. Default times are: • Less than 5 minutes, a smiley face • More than 5 minutes but less than 1 hour, a neutral face • More than 1 hour, a red frown face You can change these time by editing thresholds, as described in Editing Status Summary Thresholds on page 50
Consolidation Lag Time (Min)	Shows a graphical representation of the amount of time in minutes that the consolidotor component is behind. Times for smiley faces are the same as with Compression Lag Time above.
Local Archive Lag Time (Min)	Shows a graphical representation of the time in minutes since the last local archive operation. For less than 60 minutes a smiley face shows; for more than 60 minutes and less than 2 hours, a neutral face shows; for more than 2 hours, a red frown face shows. This does not show statistics for Centralized Archiving.
Integration Service	**Heading for a summary of Integration Service activities and processes. Shows only if System Type includes Integration Service. For detailed Integration Service information refer to Viewing Integration Service Status on page 54.**
CTI/External Links	The number of current active CTI/External links and the total number of links. This value displays as a fraction that indicates how many Integration Service links are configured for that Recorder, including active and non-active links. For example, 1/2 indicates that one link is up and one is down, out of a total of two links setup.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Recorder Connections (Active/Total)	The number of active Recorder connections to the Integration Service server PC and the total number of connections. This value displays as a fraction that indicates how many Recorder connections are configured for the Integration Service on the Recorder, including active and non-active connections. For example, 1/2 indicates that one connection is up and one is down, out of a total of two connections setup.
Active Calls being tracked	Shows the current number of recordings being tracked by the Integration Service at this time.
Active Audio Recordings being Tracked	Shows the number of active audio recordings being managed by the Integration Service at this time.
Active Screen Recordings being Tracked	Shows the number of active screen recordings being managed by the Integration Service at this time.

If there is no information for any component the field does not display.

3 Do one of the following:

- Click **Edit Thresholds** to edit status summary threshold values, as described in Editing Status Summary Thresholds on page 50.
- Click **Update** to get the latest system data and reload the page.

If you want the status at a particular instant, click **Update**.

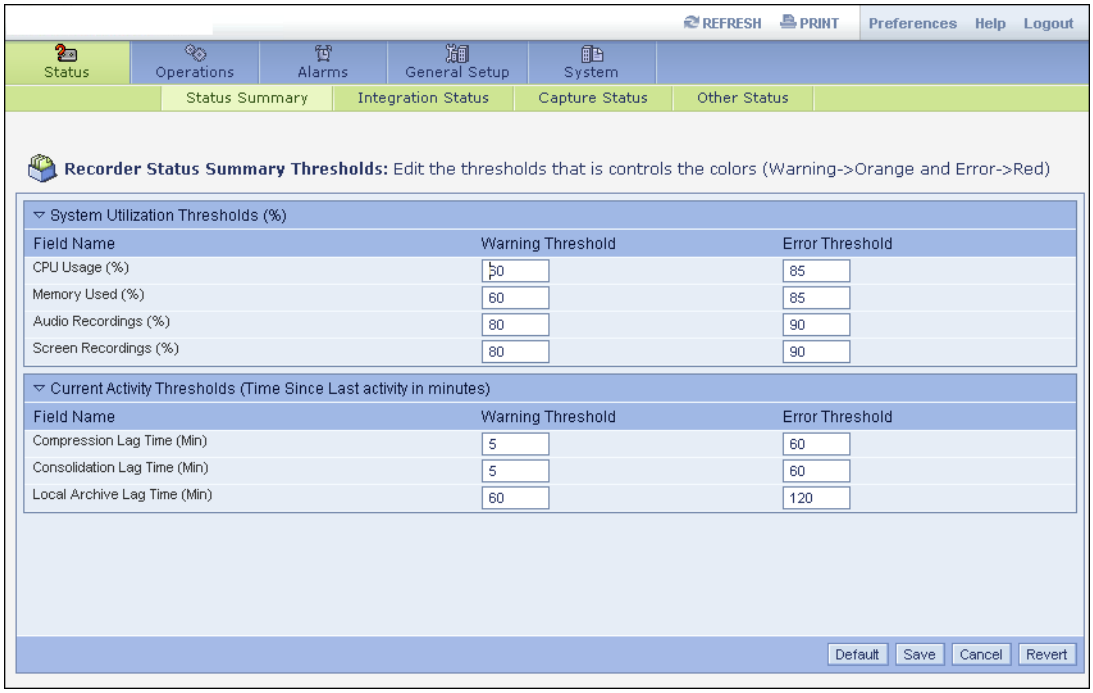
Editing Status Summary Thresholds

Edit the threshold values of status summary information to increase or decrease the point at which a warning or error displays in Recorder Manager. For example, if you set the warning and error thresholds for CPU Usage to 60 and 85 respectively, then when CPU Usage reaches 60 percent, a warning displays. When CPU Usage reaches 85 percent, an error displays, requiring that action be taken. For an explanation of each Field Names, refer to Viewing a Recorder's Status Summary on page 47.

To edit status summary thresholds:

1 Click **Status > Status Summary,** and then click **Edit Thresholds**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 In the Status Summary Thresholds window, do one of the following:

- Click **Default,** and then click **Save** to set the default values for all fields (recommended).
- Enter a number between one and 100 for Warning Threshold and Error Threshold values according to the following, and then click **Save**:

  For **Warning Threshold** type a number (see default values below) that indicates the point at which a warning displays in Recorder Manager — when the field of interest reaches this number, a warning message displays.

  For **Error Threshold**, type a number (see default values below) that indicates the point at which a warning displays in Recorder Manager — when the field of interest reaches this number, an error message displays.

Field	Threshold Default Value
CPU Usage (%) and Memory Used (%)	Warning Threshold default 60 percent.
	Error Threshold default 85 percent.
Audio Recordings (%)	Warning Threshold default 80 percent.
	Error Threshold default 95 percent.
Screen Recordings (%)	Warning Threshold default 80 percent.
	Error Threshold default 95 percent.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Threshold Default Value
Compression Lag Time (Min) and Consolidation Lag Time (Min)	Warning Threshold default 5 minutes.
	Error Threshold default 60 minutes.
Local Archive Lag Time (Min)	Warning Threshold default 60 minutes.
	Error Threshold default 120 minutes.

Viewing Capture Status

View a status summary of the Capture status, to understand how the TDM or IP capture engine in your recording system is operating. You can view statistics on two key areas: Audio Capture and Screen Capture. In this way, you can assess any potential problems and react immediately. All fields are read-only.

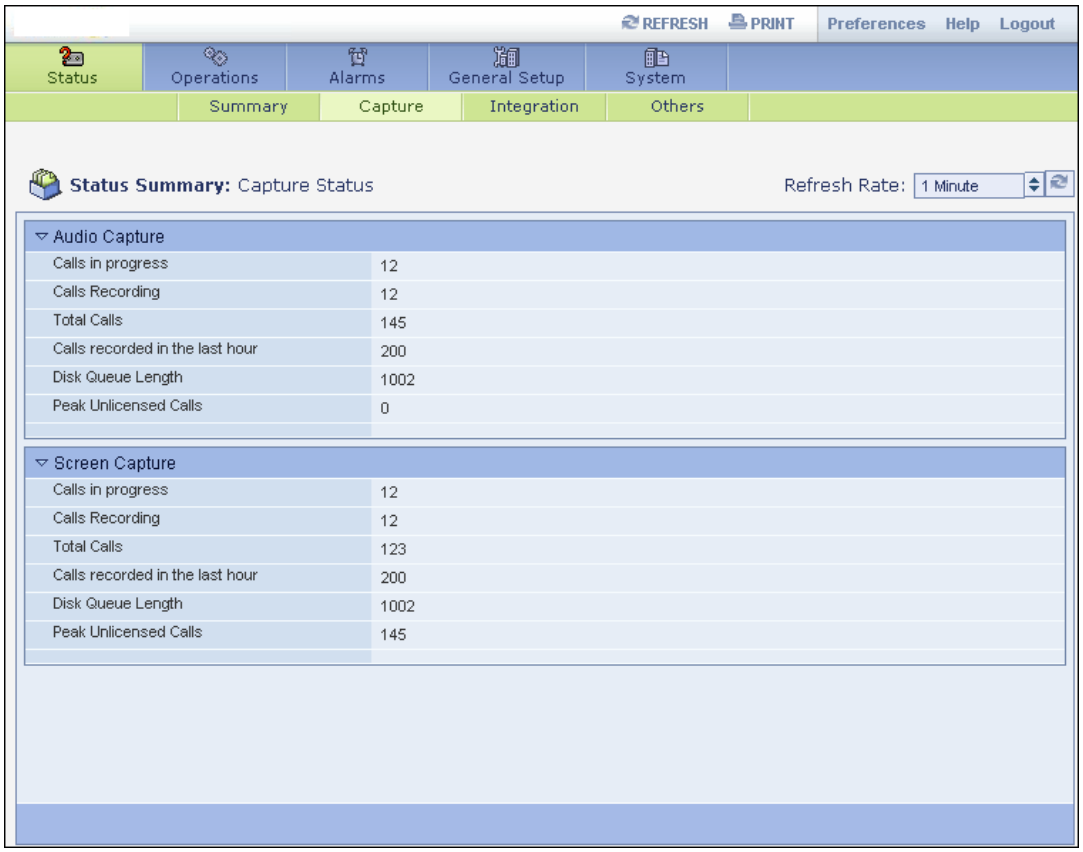
If the switch supports ITS PWE3 (IP emulation), statistics show under the TDM Recorder and not under the IP Recorder.

Tip: PWE3 is an acronym for pseudowire emulation protocol (the 3 stands for edge to edge emulation), in which services such as time frames are replaced with data packets over the same channels in the TDM trunk, as opposed to traditional IP telephony, which is RTP-based.

To view Capture Status:

1 Click **Status > Capture Status**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Review Capture Status fields according to the following:

Field	Description
Refresh Rate	Sets the refresh rate for the Capture Status screen. Values range from one minute (the default) to 20 minutes. Longer refresh rates lessen the impact on system performance.
Calls in progress *	Shows the current number of contacts that the Recorder is aware of (that is, contacts "seen" by the Recorder).
Calls Recording *	Shows the number of contacts being recorded by the Recorder.
Total Calls *	Shows the total number of contacts recorded since the last restart of the Recorder.
Calls recorded in last hour*	Shows the total number of contacts being recorded in the last hour.
Disk Queue Length *	Shows the number of contacts queued, while awaiting processing, to be placed into the Call Buffer.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Peak Unlicensed Calls *	Shows the maximum number of unlicensed contacts received at the same time. This can be helpful in many licensing scenarios to see if calls/screens in progress is greater than calls/screens recording.
* Applies to both Voice Recorder (audio capture) and Screen Recorder (screen capture)	

3 Click another tab to continue

Viewing Integration Service Status

View a status summary of the Integration Service, if installed, to understand how the Integration Service component in your Recording system is operating. You can view statistics on five key areas: Data Sources, Business Rules Engine, Recorders, Adapters, and Internal Queues. In this way, you can assess any potential problems and react immediately. All information (except the Refresh rate) is read-only.

To view Integration Service Status:

1 Click **Status > Integration Status**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

2 Review fields in the Integration Status (IS) window according to the following:

Field	**Description**
Refresh Rate	Allows you to set the refresh rate for the Integration Status screen. Values range from one minute (the default) to 20 minutes. Longer refresh rates lessen the impact on system performance.
Data Sources	**Heading for Data Sources information**
Name	Shows the name of the Data Source to which the IS is associated.
Lines (Registered/Tracked)	Shows the number of phone lines registered to, and tracked by, the Data Source.
Calls	Shows the total number of calls per Data Source.
Calls/Hour (Current/Max)	Shows the number of calls recorded in the last hour, followed by the maximum in any hour.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Events In/Hour (Current/Max)	Shows the number of Switch Events that came into the IS in the last hour, expressed as the current number compared to the maximum allowable number per hour.
Events Out/Hour (Current/Max)	Shows the number of Switch Events that are relayed from the integration service in the last hour, expressed as the current number compared to the maximum allowable number per hour.
Business Rules Engine	**Heading for Business Rules Information**
Number of Rules (Active/Configured)	Shows the number of business rules currently active and configured.
Evaluation Rate	Shows the rate at which business rules are evaluated.
Average Rules per Event	Shows the average number of rules that apply to each event.
Trigger Rate (Current/ Maximum)	Shows the calculated rate at which business rules are triggered, shown as the current and the maximum rate to date.
Recorders	**Heading for Recorder(s) Information**
Name	Lists the names of all Recorders associated with the IS.
Role	Shows the roles of the recorder. Options include: Voice or Screen Recorder, IP Analyzer, Archive, Integration Service.
Status	Shows the connection status of the Recorder. Options include Connected and Not Connected.
Last Connect Time	Shows the last time the the Recorder was connected to the Integration Service.
Recordings (Current/Max)	Shows the number of recordings currently in progress, followed by the maximum number of allowable recordings.
Message Rate (Current/Max)	Shows the calculated rate at which system messages are taking place, expressed as the current rate and the maximum message rate to date.
Recording Rate (Current/Max)	Shows the calculated rate at which recordings are taking place, expressed as the current rate and the maximum recording rate to date.
Lag (Current/Max)	Shows the Recorder’s processing lag time in seconds , expressed as the current lag time and the maximum lag time to date.
Adapters	**Heading for information about installed CTI Adapters**
Name	Lists the names of the CTI Adapter(s).
Startup Type	Shows the startup type of the CTI adapter. Options include: Automatic, Manual, and Disabled.
Status	Shows the status of the CTI adapter. Statuses include Started, Stopped, Starting, Stopping.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Last Startup Time	Shows the last time the CTI adapter was started.
Events Per Hour	Shows the rate of events being processed by the CTI adapter each hour.
Internal Queues	**Heading for Internal Queue Information.**
Name	Shows the name of the queue.
Value	Shows the number of entries in the queue.
Max Value	Shows the maximum number of entries ever in the queue.
Rate	Shows how fast items are being processed from the queue.
Max Rate	Shows the fastest rate at which items were ever processed from the queue.

3 Click another tab to continue

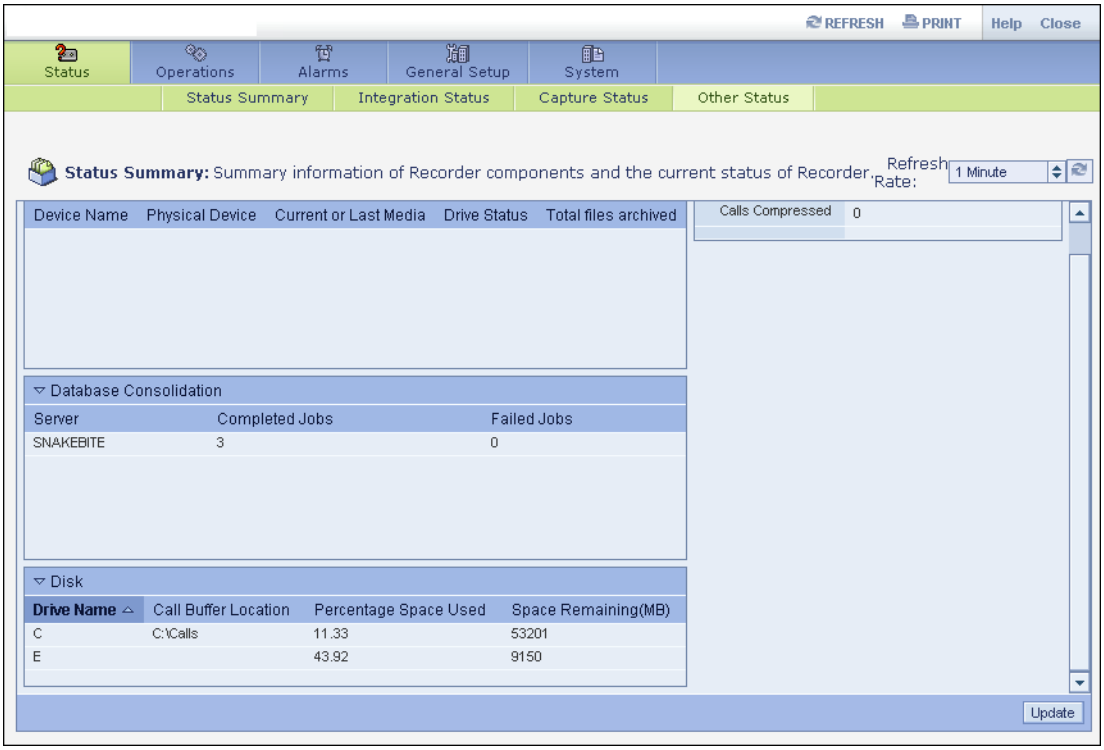
Viewing the Status of Other Components

View a status summary of remaining Recorder components to understand how these key components are operating. You can view statistics on four key areas: Archive (including Centralized Archive), Database Consolidation, Disk, and Compressor. In this way, you can assess any potential problems and react immediately.

To view the status of other Recorder components:

1 Click **Status > Other Status**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Review Other Status screen fields according to the following:

Field	Description
Archive	**Heading for information on local and Centralized Archive. For more information, refer to Configuring Archive on page 65 and Configuring Centralized Archiving on page 106.**
Device Name	Lists the names assigned in the operating system or in Windows to archive devices.
Physical Device	Shows the type of archive device, such as DVD-RW or Tape.
Current or Last Media	Shows the archive media device currently being used or last used.
Drive Status	Shows the status or the archive drive.
Total Files Archived	Shows the total number of files archived to date.
Database Consolidation	**Heading for summary of database consolidator performance. For more information, refer to Configuring Database Settings on page 79.**
Server	The logical name of the database server such as **ATL Media Server.** This is Server in the case of a SQL Server, or Net Service Name in the case of Oracle.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Completed Jobs	The number of database consolidations that have completed successfully.
Failed Jobs	The number of database consolidations that were unsuccessful
Disk	**Heading for logical disk information on the PC. For more information, refer to** Configuring Disk Manager **on page 77**
Call Buffer Location	Shows the path/location to the Recorder's Call Buffer on the disk, such as D:\Calls.
Percentage Space Used	Shows the percentage of hard disk space used for a hard drive in the list.
Space Remaining (MB)	Shows the amount of hard disk space, in megabytes (MB), not being used for a hard drive in the list.
Compressor	**A summary of compressor performance. For more information, refer to** Configuring Compression **on page 84**
Calls Compressed	The total number of contacts processed by the Compressor component.

3 Do one of the following:

- Click another tab to continue.
- Click **Update** to get the latest system data and reload the page.

  A system Update is more current than the system refresh. With system refresh, data is updated automatically according to the Refresh Rate setting. Click **Update** to obtain the latest data at a particular instant in time.

Setting up the Recorder

Set up the Recorder to start and stop components and to setup the Call Buffer. These tasks are described in the following topics:

- Starting and Stopping the Recorder and Components
- Editing Component Start and Stop Settings
- Restarting Web Services
- Configuring Recorder Settings (Call Buffer)
- Changing the Call Buffer Location
- Troubleshooting Recorder Updates

Starting and Stopping the Recorder and Components

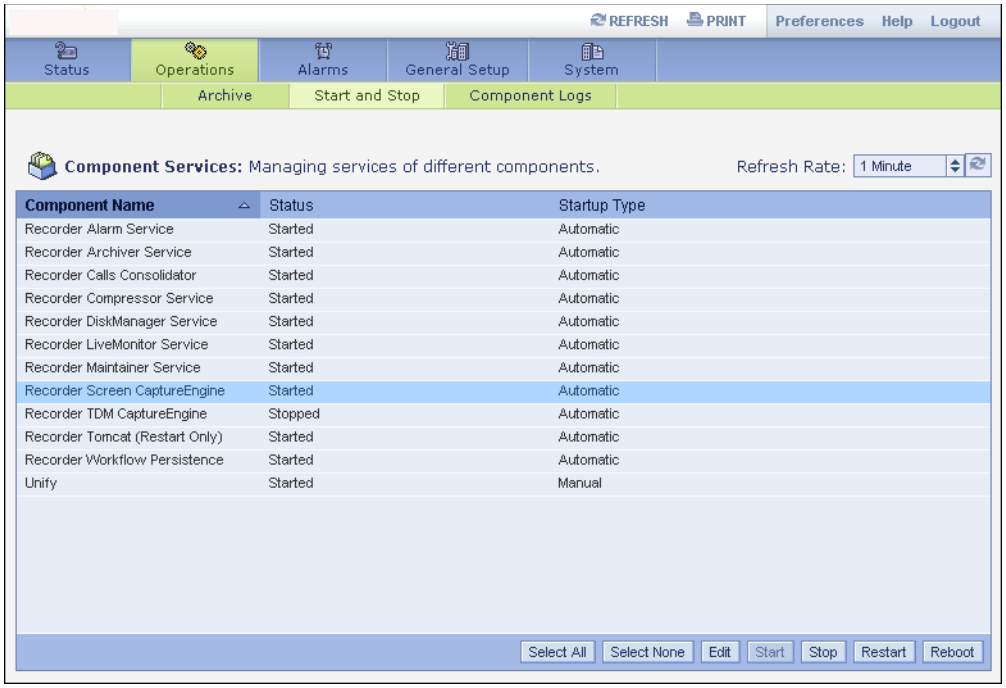
Manage the services of different Voice and Screen Recorder or Analyzer components by starting and stopping them in a controlled manner from Recorder Manager. Controlled starting and stopping allows:

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- starting and stopping of components without interrupting communication with the Recorder or Analyzer,
- reestablishing communication after a temporary interruption, such as with the Tomcat Service.

To start and stop Recorder or Analyzer components:

1 Click **Operations > Start and Stop**. The Components page displays.



2 Review the settings according to the following:

Item	Description
Component Name	The name of the installed Recorder component.
Status	The current operational status of the components, either **Started** or **Stopped**.
Start Type	The type of start/stop setting applied to the named component. Can be **Automatic** (services start automatically whenever the PC is started)**, Manual**, (services start only when the Start button is clicked by a user) or **Disabled** (services are disabled at startup, requiring that they be edited to change the Start Type before the service can be started).

3 Do one of the following:

- Select one or more components or click **Select All**, and then click **Start** or **Stop** to start or stop the selected component(s). The Start or Stop operation does not

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

execute for the **Disabled** Start Type. Start, Stop, and Edit options are not available for components that require a restart.

- For components that cannot be started or stopped, such as Tomcat Services, click **Restart** to restart that component.
- Click **Reboot** to reboot the server.

  Caution: Rebooting the server should be done only as a very last resort, as contacts being recorded or other unfinished processes may be lost.

Editing Component Start and Stop Settings

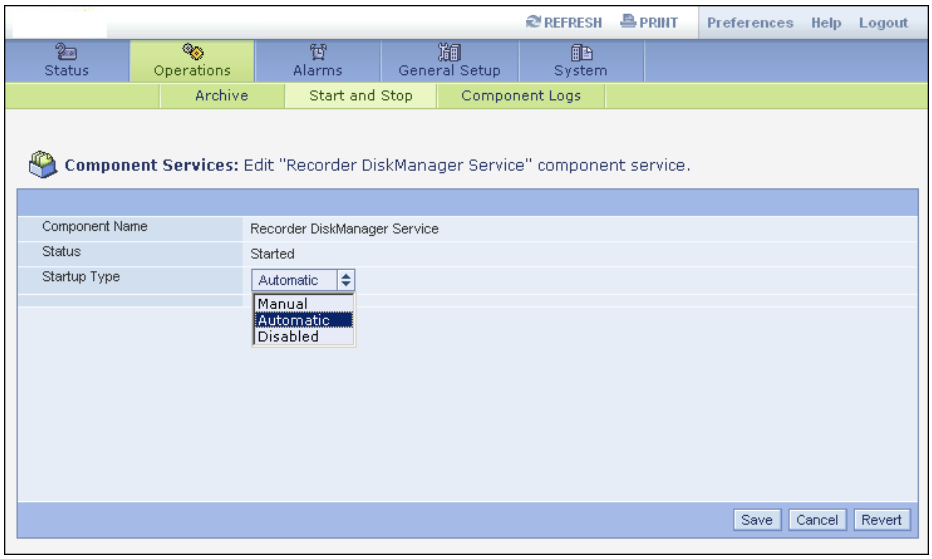
Use the Edit Component option to change Startup Type of individual components. Possible values are Automatic, Manual, or Disabled. Tomcat service is a Restart only component. Restart only components cannot be edited.

If you are working from Enterprise Manager, verify that your security permissions include editing individual Recorder components within the Recorder Manager.

To edit the start/stop type of a component:

1 Choose **Operations > Start and Stop,** and then select a component.

2 Click **Edit**. The Component Service Details window displays.



If the Edit button is disabled, then the component cannot be edited or you do not have sufficient security privileges. For example if you are logged in from Enterprise Manager and you do not have Edit privileges, the Edit button is disabled.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 For Startup Type, choose a setting according to the following:

Item	Description
Automatic	The service of the component starts automatically when the system is started. For example, if the system is rebooted, service to the component starts automatically upon the reboot.
Manual	The service of the component must be started manually by selecting the component in the Start and Stop/component window and clicking **Start**.
Disabled	The service of the component cannot be started either automatically or manually. The component remains disabled until the **Start Type** is changed to **Automatic** or **Manual**.

4 Click **Save**.

Restarting Web Services

Restart web services manually when Recorder Manager or Tomcat fails to connect automatically to the Recorder's web services.

To restart web services manually:

1 Launch Recorder Manager as normal. If RM/Tomcat starts up but cannot connect to Recorder web service for some reason, the Server Roles error window displays.

2 Click **Operations > Start and Stop**. The Recorder component services window displays.

3 Click the **Recorder Tomcat** component, and then click **Restart**. Refer also to Starting and Stopping the Recorder and Components on page 59.

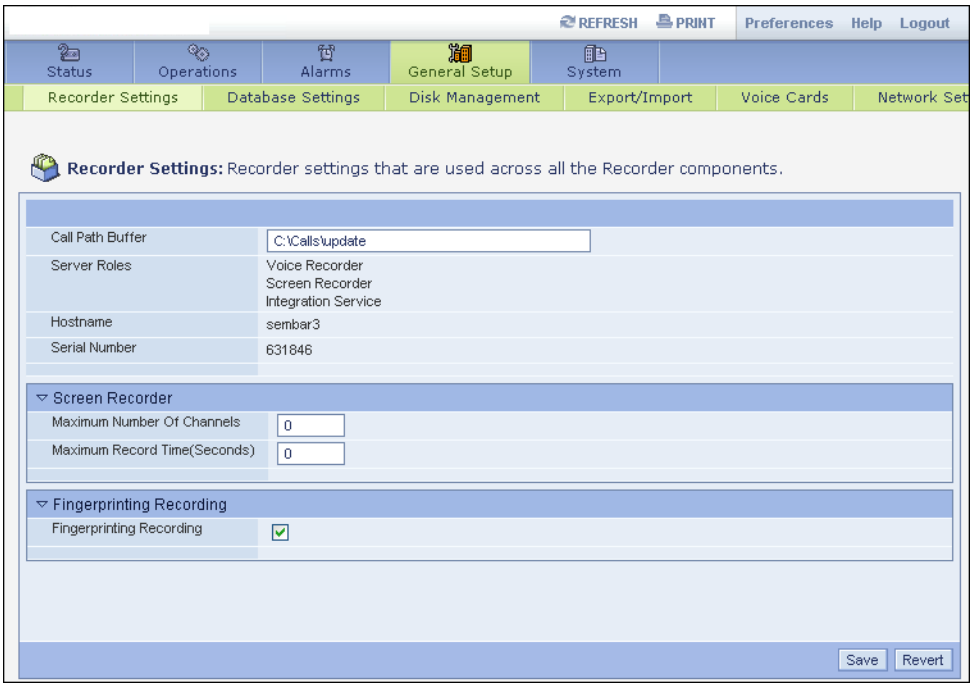
Configuring Recorder Settings (Call Buffer)

Configure Recorder settings to tell the Recorder the disk storage area (the Call Buffer, also known as the calls cache) where calls will be saved when first recorded. As the Call Buffer fills up, calls are copied automatically to more permanent storage, depending on your threshold and archive settings. Disk Manager begins deleting the oldest calls from the Call Buffer once a specified disk threshold is reached.

To configure Recorder settings:

1 Click **General Setup** > **Recorder Settings**. The Recorder Settings window displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 For **Call Buffer Path**, type the path to the Call Buffer, such as **`D:\Calls`**. It is recommended that the Call Buffer be located on a different drive from system files.

If you later change the location of the Call Buffer, refer to Changing the Call Buffer Location on page 64, otherwise Search and Replay may not be able to find and replay some calls.

3 Review **Server Role**, **Hostname** and **Serial Number** fields. These fields are read-only, representing the functional roles for this Recorder, the host name of the server, and the serial number of this Server respectively.

4 Check **Fingerprinting Recording** to indicate that configuration files will have a checksum digit inserted so that any file that has been manually edited (that is, tampered with) can be detected and corrected. An alarm is triggered when a tampered file is detected. To correct a checksum mismatch, refer to Correcting Checksum Mismatches on page 259. For more information on overall system security, refer to the *Enterprise Security Administration Guide* in the documentation folder of your install CD/DVD.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

5 In the **Screen Recording** area, which is visible only if the Recorder has a Screen Recorder role, complete the fields according to the following:

Item	Description
Max. no. of channels	Type the maximum number of concurrent channels available for screen recording, as determined by your license, or accept the default 50. Screens are not recorded after this limit has been reached.
Max record time (secs)	Type the maximum time, in seconds, for the recording of screen data, or accept the default of 1800 seconds. After this time, screen recording stops.

6 Click **Save**.

Changing the Call Buffer Location

Change the Call Buffer location to assign a different initial hard disk location for recorded contacts from the disk location specified at installation. Other tasks are involved in changing the location. You must manually move files from the old to the new location after stopping all recording components and then direct components to use the new location. It is recommended that all tasks be performed at a time other than normal business hours.

To change the Call Buffer location:

Change the Call Buffer location to move all files in the old Call Buffer into a new location.

1 Choose **Operations > Start and Stop** to stop all Recorder components except web service.

2 Launch Windows Explorer and create the new Call Buffer directory on the PC's hard disk.

3 In Windows Explorer, move all files and subfolders from the old Call Buffer folder to the new Call Buffer folder. (This may take some time if the old Call Buffer is large.)

4 Use Recorder Manager to change the Call Buffer path to point to the newly created one, as described in Configuring Recorder Settings (Call Buffer) on page 62.

5 Choose **Operations > Start and Stop** to restart all the components

To assign a new Call Buffer location:

Assign a new Call Buffer location to retain files in the old Call Buffer while using a new Call Buffer working location. This would be necessary if copying the content form the existing Call Buffer to the new Call Buffer is not possible. For example, a new drive may be added that is the same size as the existing one.

1 Choose **Operations > Start and Stop** and stop the Capture engine after ensuring that its persist queue to workflow is empty.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

2 Choose **Operations > Start and Stop** again to stop all other Recorder components except web service after ensuring that they have processed all the records in workflow database.

3 Create the new Call Buffer as described in To change the Call Buffer location: on page 64.

4 Change the Call Buffer directory using Recorder Manager as described in Configuring Recorder Settings (Call Buffer) on page 62 to point to the new Call Buffer

5 Choose **Operations > Start and Stop** to restart all the components.

Tip: The drawback to assigning a new Call Buffer location is that you cannot replay the contacts recorded and stored in the old Call Buffer location, although the contacts are still present. You may not be able to play back these contacts, unless they have already been archived.

Troubleshooting Recorder Updates

If the component cannot be updated, do the following troubleshooting:

- Check that an active network connection exists
- Check that you have security privileges to make the change
- Check that the recording subsystem is installed correctly
- Make sure that Recorder Web Services are up and running
- Check that the Call Buffer location has not been changed. See Changing the Call Buffer Location on page 64

Configuring Archive

Configure Archive to create and manage drives that copy files from Recorders to storage media. Individual drives can be configured to archive all contacts (.WAV, SCN, and .XML files) on the local Recorder, or to archive a campaign-driven set of contacts pulled from remote Recorders (known as enterprise Archive, central Archive, or remote archive, as described in Configuring Optional Components on page 93).

The Archive process does not remove contacts from the Recorder's call buffer; it only replicates the contacts from the call buffer to other storage. It is the Recorder's Disk Manager that monitors the call buffer and deletes the oldest contacts when space is needed for newly recorded contacts. A Recorder writes to the archive device each time there are 100MB of calls that have finished recording. If it has not built up 100MB in one hour since the last time it has written, then it writes what has been gathered so far.

You can add a new archive drive, edit archive settings, and delete drives. You can also eject media, print labels, and reformat removable media. These tasks are described in the following topics:

- Managing Archive Drives
- Configuring an Archive Drive
- Configuring General Archive Settings

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

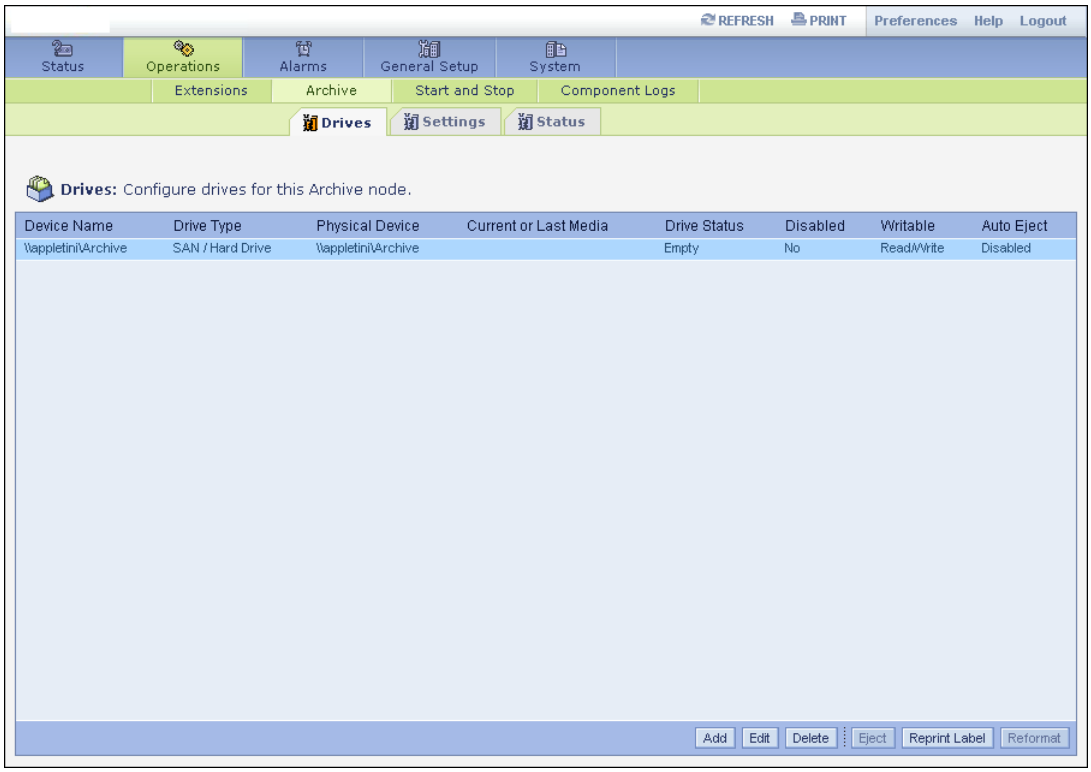
- Disabling Archive Failover Alarms
- Replacing a Physical Archive Device
- Reviewing the Status of Archiving Operations

Managing Archive Drives

Manage archive drives in the drive management window to view, add, edit, or delete configured drives. You can review current settings from the drive management window, as well as eject a removable media, reprint a label, reformat a removable media, or edit settings on any device. You can manage local archive drives and centralized archiving drives if installed.

To access drive management on a Recorder:

1 In the Recorder Manager click **Operations** > **Archive > Drives**. The Archive window displays all registered archive devices.



2 Review fields according to the descriptions in Configuring an Archive Drive on page 67.

3 Do one of the following:

- Click **Eject** (when enabled) to eject the selected removable media.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Ejection may take some time as the archive medium must finish its current process so that data is not lost.

- Click **Reprint Label** to send an instruction to the Label printer, if attached, to reprint the label for the last-used archive media.
- Click **Reformat** to format an archive removable media.
- Click **Add** to add an archive drive, as described in Replacing a Physical Archive Device on page 74.
- Click **Edit** with the drive selected to go to the Configure a Local Archive Drive window to setup the drive, as described in Configuring an Archive Drive on page 67.
- Click **Delete** to remove the drive configuration

Notes:

- CD ROMs are not supported as local archive devices.
- For previous releases, if your DVD-RAM is not recognized, check the Archiver logs to show what Archiver reads as the firmware name of the device (such as MATSUSHITA DV3904). Copy this name and open ARCHIVERCONFIG.XML. Paste the name into the DeviceType Description field, and then also change the device type number. Once saved, restart the Archiver service. For the current release, the different DVD media formats are automatically recognized.

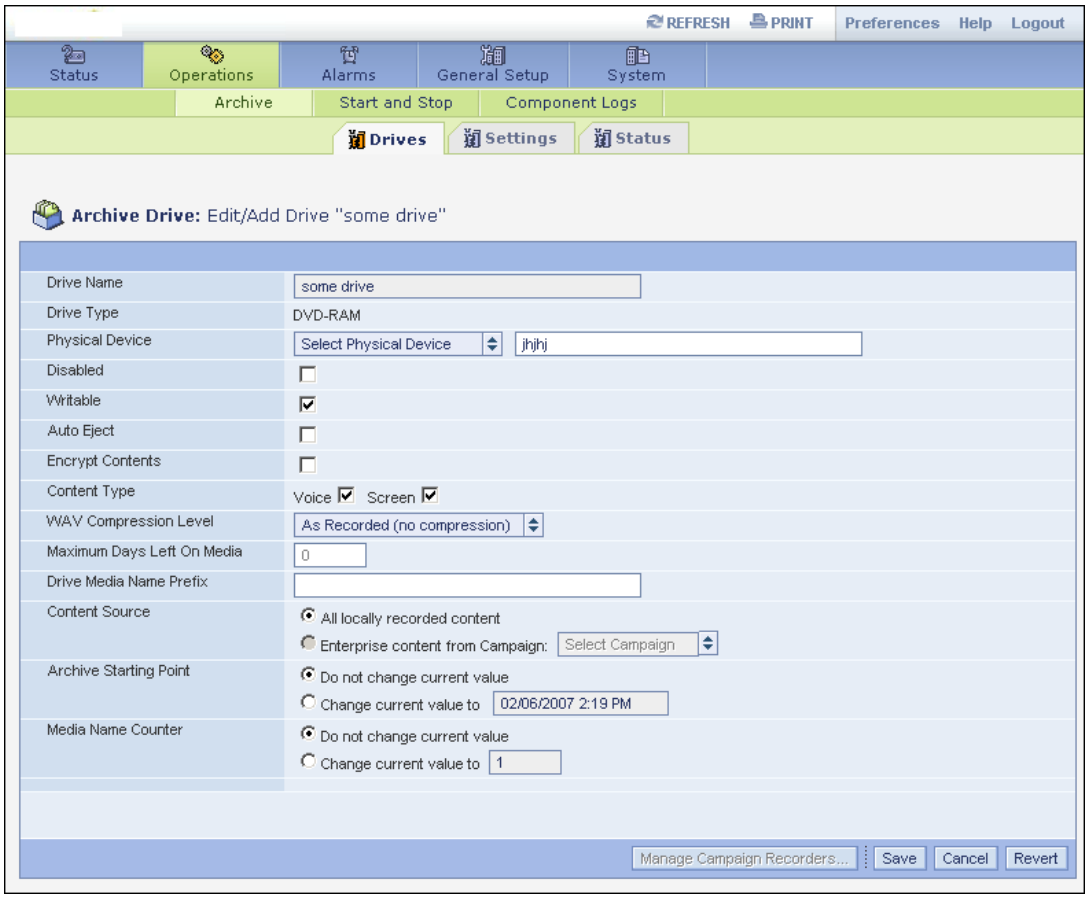
Configuring an Archive Drive

Configure archive drives to specify how and where to copy files for long-term storage. Each drive may operate in Local or Enterprise mode. Local archive drives copy 100 percent of all files from the local Recorder's call buffer to the specified archive drive. Enterprise archive drives run campaigns to pull selected content from remote Recorders. This process is described in the *Centralized Archiving Installation and Administration Guide*.

To add a new or configure an existing local archive drive:

1 Choose **Operations** > **Archive > Drives,** select any drive, and then click **Edit** (or click **Add** to simply add a new drive).

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Edit the local archive drive details according to the following:

Item	Description
Drive Name	The user-editable name of the drive being used for the archiving of contacts, such as **DVD Home**. You will assign an actual device to this drive name when you complete the Physical Device area below.
Drive Type	The type of the storage device, such as Tape, DVD, or EMC Centera. Other options include DVD-RAM, DVD+/-RW, IOMEGA REV drive. Different DVD media formats are recognized automatically. **Note**: If you are using a USB DVD archive device, writing may be unstable. It is recommended that you test with the DVD Validator utility located on the installation DVD.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Item	Description
Physical Device	The selection box (left field) contains local physical devices attached to the Archive system. If the Drive Type is one of the removable media (such as DVD or Tape) then select one of the locally attached devices as the archival target. Once selected the local device's information is automatically propagated to the edit box (right field) as well. If the Drive Type is one of the fixed, remote drives (such as SAN or EMC Centera) then the edit box should be manually updated to contain the connection string to that storage device. In the case of a SAN, the connection string could contain the UNC path to the target file share, for example **\\computername\sharedfolder**. Note that Archiver is a Windows service that runs by default under the LocalSystem account. If any special permissions are needed to read and write to the target UNC path then the Archiver service account should be changed to one that has those permissions. For EMC Centera drive types, the connection string should contain a valid Centera path (typically an IP address or hostname). See examples in EMC Centera Connection String Examples on page 70. **Note**: You may assign different physical devices to the drive name over time as drives are replaced and the settings will stay the same for the new physical device.
Disabled	Checkbox that allows you to disable an archive drive so that it cannot be used. A drive that is disabled will not archive contacts or support replay requests.
Writable	Checkbox that allows you to make the drive Writeable or Read-Only. Writeable drives are used only to archive new data. Read-Only drives are used only to play back files from existing media. The writeable option can only be changed when the Drive has a status of **Empty**. An alarm is triggered if a write-protected media is inserted into a Writeable drive. **Note**: For Recorders that do not have writable local archive devices the device should be set to read-only by unchecking the writeable check box for the archive device.
Auto Eject	Checkbox that if enabled (checked) will cause the media to be ejected automatically when the media is 100 percent full, or if disabled (unchecked) will cause the media not to be ejected automatically when it detects that no more media capacity is available. **Tip:** If the drive has a non-archive media in it such as a regular CD-ROM it displays an UNKNOWN status. The unwritable medium should be ejected.
Encrypt Contents	Specifies if new files archived to the drive should be encrypted, if encryption is supported. For more information on encrypting archive data (.wav and .xml files) refer to the *Enterprise Security Administration Guide*.
Content Type	Choose one or both of **Voice** or **Screen** content types as follows: • Choose **Voice,** to archive phone calls from designated extensions. • Choose **Screen** to archive screen captures from designated workstations.
WAV Compression Level	Choose the type of compression for recorded audio files. Choices include No compression and Compress to G.726 (2 kb/sec), which is the standard audio compression format for the Recorder.
Maximum Days Left on Medium	Optionally enter a number representing the maximum number of days that the recording has to be left on the archive medium.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Item	Description
Drive Media Name Prefix	Part of the media name for media recorded on this drive. Used as label information also.
Content Source	Do one of the following: • Check **All locally recorded content** to perform archiving operations on all contacts recorded on the local Recorder. • Check **Enterprise content from Campaign** to peform centralized archiving from the specified campaign to this drive. For more information, refer to the *Centralized Archiving Installation and Administration Guide* supplied with your Archive software (obtained separately).
Archive Starting Point	The date and timestamp at which archiving will begin in the next cycle. For newly added devices some valid starting point MUST be selected. Choose the current time to begin archiving new contacts, or choose some earlier time to archive pre-existing contacts in the online buffer.
Media Name Counter	Integer index from 00001-99999 that forms the next media name. Used as label information also.

If archive devices are changed, for example a new device added with a new name, then old alarms may need to be cleared manually in the Recorder Manager as they will not be cleared automatically.

3 Click **Save.**

If a system message advises you to restart the Archive service, click **Operations > Start and Stop** and restart the Archiver component.

4 If you have Centralized Archiving installed, the **Manage Campaign Recorders** button is enabled. Clicking this button opens a window listing Recorders that can be added to a campaign. This information is described in Configuring Centralized Archiving on page 106.

EMC Centera Connection String Examples

The following are examples of connection strings that can be used with EMC Centera. Refer also to the EMC Centera user documentation for the latest details:

```
pooladdress ::= hintlist

hintlist ::= hint ("," hint)*

hint ::= [ protocol "://" ] ipreference [ ":" port ]

protocol ::= "hpp"

port ::= [0-9]+ (default is 3218)

ipreference ::= dnsname | ip-address

dnsname ::= DNS name is a DNS maintained name that resolves to one
or more IP addresses (using round-robin) max length is 256 chars

ip-address ::= 4-tuple address format
```

A hint is a single pool address and a hintlist contains one or more hints.

Profile Information

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

You can augment the connection string with the PEA file or username/secret for the PAI module to be used by the application. For example:

```
"10.2.3.4,10.6.7.8?c:\centera\rwe.pea"
```

or

```
"10.2.3.4,10.6.7.8?name=<username>,secret=<password>"
```

You also can assign multiple profiles on a connection string to access one or more clusters. For more information on PAI modules and the syntax of connection strings, refer to the *Centera Programmer's Guide*, P/N 069001127.

Connection Failover Prefixes

Addresses prefixed with primary=, called primary addresses, are eligible for becoming the primary cluster. Addresses prefixed with secondary=, called secondary addresses, are not eligible for becoming the primary cluster. An address without a prefix is a primary address. For example:

```
"10.2.3.4,primary=10.6.7.8,secondary=10.11.12.13"
```

Both **10.2.3.4** and **10.6.7.8** are primary addresses, and **10.11.12.13** is a secondary address.

If all primary connections for nodes with the access role fail, the **FPPool_Open()** function fails. The **primary=** and **secondary=** prefixes are case-sensitive, and there can be no whitespace before or after the equal sign (=). Refer to *Multicluster Failover* in the *Centera Programmer's Guide*, P/N 069001127, for more information on connection failover.

API Reference

This example specifies a connection string with multiple IP addresses—a best practice that protects against one or more nodes with the access role of a cluster being unavailable.

```
myPool = FPPool_Open
("10.1.1.1,10.1.1.2,10.1.1.3,10.1.1.4");
```

This example opens a pool using the specified PEA file.

```
myPoolName = "10.62.69.153?c:\centera\rwe.pea";
```

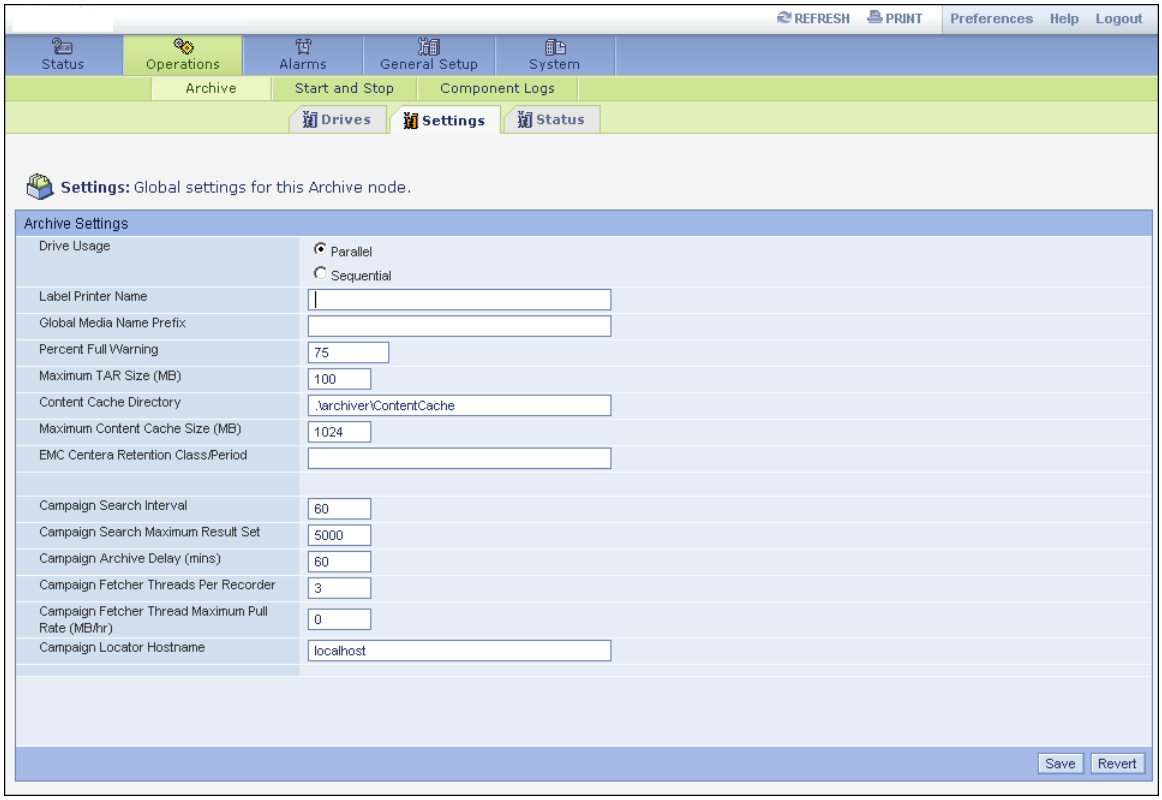
Configuring General Archive Settings

Configure general archive settings to adjust parameters that impact overall Archive behavior and all configured drives.

To configure general archive settings:

1 Choose **Operations** > **Archive > Settings**. The Archive settings screen displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Complete the fields according to the following table:

Item	Description
Drive Usage	Choose the mode (Parallel or Sequential) to be used for this archive drive. • Choose **Parallel** if you want your archive drives on this server to operate independently of each other. This applies if you want to make duplicate archive copies to different media or if you have configured archive drives that are doing different things, such as one archives audio recordings to location A, another archives screen recordings to location B. Parallel is the default and recommended setting. Choose Parallel if you have Centralized Archiving. • Choose **Sequential** to use archive drives one after the other so that archive data is always appended until the current drive is filled before moving to the next drive. Choose Sequential if you would rather not have to visit the machine as frequently to change tapes. Then Archive writes to one device until it is filled then moves on to the next device. Sequential is applicable if you have only local-mode drives configured on this system! **Note**: To change an archive mode, all drives must be empty.
Label Printer Name	The name of the printer, if present, used to create labels for the archive media.
Global Media Name Prefix	Unique prefix used in forming the media name for all drives in this Recorder.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Item	Description
Percent Full Warning	The threshold, expressed as a percentage, at which an alarm is raised. For example, if 75 is entered, an alarm displays when the media is 75 percent full, so that you can prepare to change the media.
Maximum TAR Size (MB)	The maximum size for the TAR (acronym for tape archive) file in megabytes, to be written to the media.
Content Cache Directory	Specify the directory location where contact content files are stored after retrieval from remote Recorders. The Content Cache also stores files recently requested for replay from an archive medium. The Contect Cache is managed as a circular buffer to ensure that the Maximum Content Cache Size (see below) is available at the specified location.
Maximum Content Cache Size (MB)	Type the maximum size in megabytes of the Content Cache. The larger the cache, the greater the amount of contact recording data can be queued temporarily.
EMC Centera Retention Class/ Period	Optionally type a numeric value to set a retention period or an alpha-numeric value to set a retention class (which must be pre-configured on the EMC Centera cluster). If the value is blank then no retention class or period is set. EMC Centera drive configurations on this archive server use this optional value to set a retention period or class on files archived to the cluster. For more information on retention concepts, please refer to your EMC Centera documentation.
Additional Global Settings for Centralized Archiving (The following fields should rarely be changed; most are for performance tuning.)	
Campaign Search Interval	Controls how frequently, in seconds, the search thread for each Archive drive will query Recorders for new jobs.
Campaign Search Maximum Result Set	Controls how many jobs will be returned from the query for each Recorder.
Campaign Archive Delay (mins)	Sets a minimum age of a call before it is picked up by the archive search query. Setting a delay interval allows normal post-call updates to happen before the call is first archived. Updating a call after it is archived will trigger re-archival of the call.
Campaign Fetcher Threads Per Recorder	Each drive uses a dedicated set of threads to pull call content from remote Recorders. This setting adjusts the number of threads used.
Campaign Maximum Pull Rate Per Recorder (MB/hr	If desired, setting this value limits how many megabytes (MB) are pulled from each Recorder per hour. If zero, the Recorder contacts will be pulled as fast as possible.
Campaign Locator Hostname	Specifies the hostname where the Adapter/Locator component was installed. During typical installs, the Adapter/Locator is installed on the same machine as enterprise Archive, so hostname should be left as localhost.

3 Click **Save.**

If the help message advises you to restart the Archive Manager, click **Operations > Start and Stop** and restart Archiver.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Disabling Archive Failover Alarms

A Recorder automatically raises an alarm if it detects any files in the call buffer that have gone unarchived after 7 days. It also raises an alarm when it deletes an unarchived file from the call buffer. These alarms are components in the archive failover feature, which applies to both local and central archive. If you do not have some combination of local or Centralized Archiving running to archive the Recorder's call buffer files, then you should disable this feature to avoid unnecessary alarms.

To disable archive failover alarms:

1. Load the **DiskManagerConfig.xml** file from the ContactStore directory into a text editor.
2. Change the <**AlarmIfNotArchived**> and <**NumDaysToAlarmAfter**> elements to **false** and **0** as follows:

```
<AlarmIfNotArchived>false</AlarmIfNotArchived>
<NumDaysToAlarmAfter>0</NumDaysToAlarmAfter>
```

If the above line(s) are not present, then you must add them immediately before the final <**/DiskManager**> line.

3. Save the modified **DiskManagerConfig.xml**.
4. Restart the Disk Manager service.
5. Acknowledge the file tampered alarm in Recorder Manager. The File Tampered alarm is raised because a configuration file has been modified by hand.
6. Re-save the Disk Manager settings in Recorder Manager. This step updates the configuration file with a new, valid checksum.

Replacing a Physical Archive Device

Replace a physical device to correct an archive hardware failure or to upgrade the archive device. The new physical device can be associated with the existing drive name to maintain all of the settings of the previous physical device.

To replace an existing physical device with a new device:

1. Select the target archive drive in the drive management window, and then click **Edit**.
2. Change the **Physical Device** field from the current value to empty, and then click **Save**.
3. Physically remove the old local archive device and add the new local archive device.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

4. If installing the new device required the system to reboot, then the new drive has already been auto-detected by Archiver. Otherwise, click **Operations > Start and Stop** and restart Archiver. This causes the new drive to be auto-detected.
5. Edit the target drive again from the drive management window, and then select the new physical device to be associated with the logical drive name. Windows may use the same physical device name as the replaced device or generate a new one.
6. Click **Operations > Start and Stop** as prompted and restart Archiver. The new drive settings take effect and the local archive drive is now operational.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Reviewing the Status of Archiving Operations

Optionally review the Status of Archiving to obtain information about the overall archiving process on the Recorder.

To review the status of archiving operations:

1 Choose **Operations** > **Archive > Status.** The Archive Status window displays.

2 Review the fields according to the following:

Item	Description
Drive Name	The name of the drive being used on the indicated Recorder for the archiving of contacts, such as **`ATL-Tape 2.`**
Recorder	The name of the Recorder from which the recording originated.
Write Statistics	Summary of write operations for each Recorder, including files processed, last archiving job details, data transfer rate in megabytes per hour, and number of remaining jobs.
Replay Statistics	Summary of replay statistics for the Recorder, including number of replays, last archiving job details, and replay times.

3 Click another tab to continue.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Disk Manager

Configure the disk manager component to assign Call Buffer disk settings and logical drives to the contact recording environment. The Call Buffer, also known as the calls cache, is the local disk space where the contact being recorded is stored. Once on the Call Buffer, the location of the contact is registered for later search and replay. Once the contact is deleted from the Call Buffer (i.e. when the Call Buffer threshold is reached) the contact is moved to an archive device.

This information is described in the following topics:

- Creating Disk Manager Settings
- Viewing Disk Drives

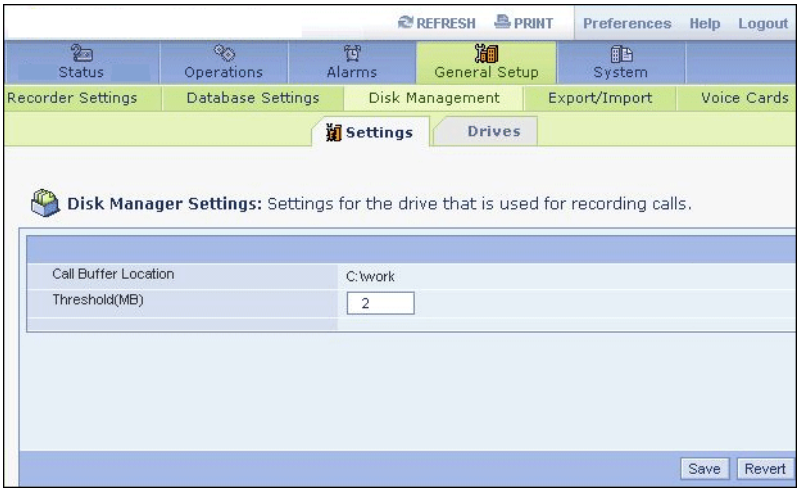
See also disk management maintenance tasks at Performing Disk Management on page 222.

Creating Disk Manager Settings

Type disk manager settings to assign drives, folders, and capacity thresholds for the recording of contact details on the local Call Buffer. Recorded contacts are stored temporarily in the Call Buffer until the specified Threshold is reached, at which time contacts are deleted from the Call Buffer, oldest first, and moved to archive storage. Until deleted by Disk Manager to free up space, contacts appear in both the Call Buffer and in archive (if configured).

To create disk manager settings:

1 In the Recorder Manager, click **General Setup > Disk Management > Settings**. The Disk Manager Settings screen displays.



2 Complete the Disk Manager Settings fields as follows:

- **Call Buffer Location**, this is a read only field showing the path to the Recorder's Call Buffer.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- For **Threshold (MB)**, type a size in megabytes for free disk space on the Call Buffer. A minimum of 2GB is recommended for smaller systems and a minimum of 50GB for systems with more than 120 channels. As a general rule, the threshold should be set at 10 percent or 10 GB whichever is smaller, so that 10 percent of the hard disk space or 10 GB is always free. This provides a tolerance level for Disk Manager to delete contacts during high volume recording when the Call Bufer fills up faster than contacts can be deleted.

3 Click **Save**.

Viewing Disk Drives

View drives managed by Disk Manager to see a list of all drives and whether alarms are to be raised (that is, monitored) when the threshold is reached. Monitoring drives ensures, for example, that the database drive or the logs drive do not run out of space.

Only one of the listed drives contains the Call Buffer. The Call Buffer drive is the only drive from which the Disk Manager deletes old files. It is recommended that this drive be at least 2GB in size for smaller systems and 50 GB (minimum) for systems recording 120 channels or more.

To view disk drives:

1 Click **General Setup > Disk Management > Drives**. The Monitor Drives screen displays.

2 Complete the Monitor Drives fields as follows:

- For **Threshold (MB)** optionally type the number of megabytes beside each Drive for the threshold. When disk space on the drive reaches the threshold size, these drives are monitored through alarms being triggered.

  If the **Monitor** field is checked, the **Threshold** field becomes enabled and mandatory, requiring you to type a threshold value greater than zero.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- Under **Monitor**, click to place a checkmark to indicate that the drive is being monitored, in which case an alarm is raised when the threshold is reached. If checked, a value must appear in the **Threshold** field.

3 Click **Save**.

Configuring Database Settings

Configure the Recorder's database settings (consolidator) to identify a database server by giving it a name and to authorize the database for media consolidation. Media consolidation is the process of copying the location of the contact's audio (that is, the **`.wav`**) file for calls, screen (that is **`.scn`**) file for screen captures, and metadata (that is, the **`.xml`**) file to the media database and calls database respectively. At installation, a single database server with the media consolidation option checked is created. You can then add a second database server as well as edit and delete.

If you use Windows 2003 server or one or more applications that access SQL 2005, you need the appropriate Client Access Licenses (CALs). This ensures compliance with Microsoft's licensing agreement. Please review CAL requirements in your system documentation before installing Microsoft products, or refer to http://www.microsoft.com/windowsserver2003/howtobuy/licensing/caloverview.mspx.

Information is presented in the following topics:

- Viewing Database Settings
- Creating a Database Server
- Editing a Database Server
- Deleting a Database Server

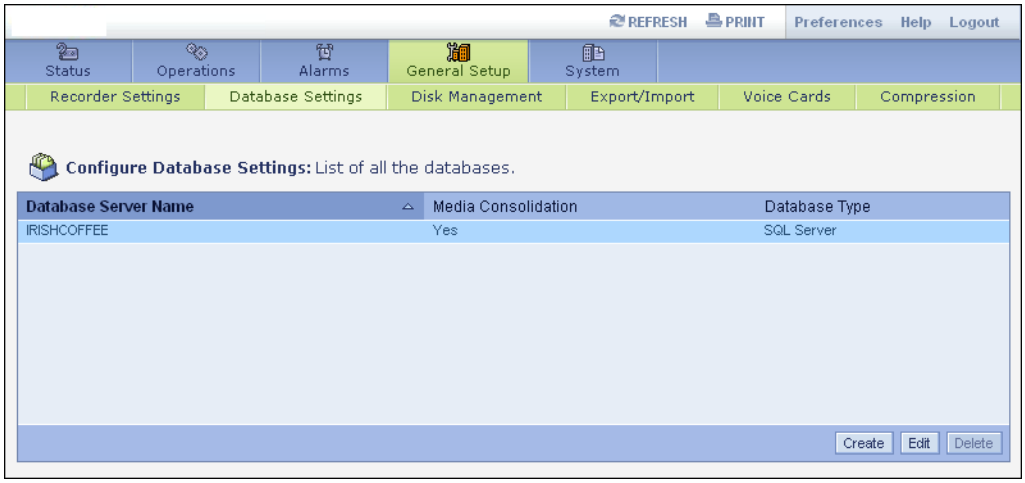
Viewing Database Settings

View database settings to view databases that have been set up, and to access tools for creating, editing, and deleting database servers. Select a database to edit or delete it. The create option is available only if a second database is to be created. A maximum of two databases, one of which must have media consolidation enabled, can be displayed.

To view and edit database settings:

1 In the Recorder Manager click **General Setup > Database Settings**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Review the fields according to the following:

Field	Description
Database Server Name	Shows the name of the database server. This name must be unique.
Media Consolidation	Shows whether there is a media consolidation with the associated server, in which case call data and audio data are linked. At least one database server must have media consolidation enabled.
Database Type	Shows the type of database (read-only). You cannot change the database type.

3 Do one of the following:

- Click **Create** to open a blank database settings window and type the name of a new database server. See Creating a Database Server on page 80.
- Click **Edit** with a database selected to type a new name or choose a different media consolidation. See Editing a Database Server on page 82.
- Click **Delete** to delete a selected database server. See Deleting a Database Server on page 82.

Creating a Database Server

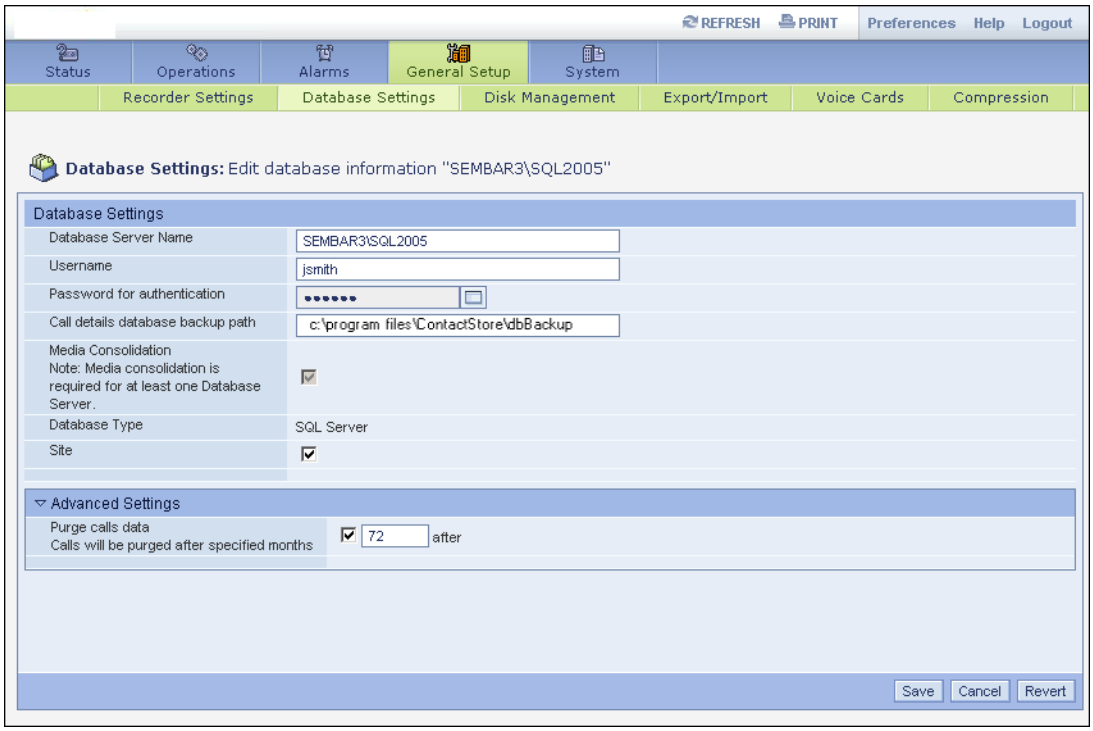
Create a database server to provide the profile of a second database server (only two are permitted) and to determine if it will be used for consolidating the call's media and data files. Media consolidation is possible on one database server only. You must restart the Recorder before any changes take effect.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To create a database server:

1 In the Recorder Manager with one database created, click **General Setup > Database Settings,** and then click **Create**.

Note that you cannot create more than two database servers. The Create button is disabled after two database servers have been created.



2 Complete the Database Settings fields according to the following:

Item	Description
Database Server Name/NetService Name	Type a unique, descriptive name for the database server. The field is labelled **Database Server Name** if an SQL server is installed. If you are using a SQL2005 database, you must provide a server name along with the instance, such as **`Servername\SQL2005`**.
Username	Type the username for accessing the database being created.
Password for authentication	Set the password to access the database (this may be the same as the password created at installation) by clicking the password icon at the end of the row.
Call details database backup path	Type the folder where the database is to be backed up on the server. The backup process is done automatically by the system. This applies to SQL Server only. If an Oracle database is being used, this field does not display.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Item	Description
Media Consolidation	This field is disabled and checked if there are no other media consolidators setup. At least one database must be enabled for media consolidation.
Database Type	Shows the type of database. This field is read-only.
Site	Check this field to indicate if this database is a Centralized Archiving Site Database. If any Centralized Archiving drives are configured there must be one site database setting enabled on this server.
Purge Calls Data (Advanced Settings)	Shows when contact data files are to be deleted (that is, purged) automatically by the Consolidator component. If this field is checked, you must type in the number of months, default 360 (30 years). If unchecked, the contacts will not be deleted. The Consolidator component deletes contact data based on this setting, regardless of which Recorder recorded the contacts. If multiple Recorders are configured to consolidate to a single database, it is recommended that only one of these Recorders have this setting configured to avoid conflicting settings.

3 Click **Save**.

4 When prompted, restart the Recorder, as described in Starting and Stopping the Recorder and Components on page 59.

Editing a Database Server

Edit a selected database server to change any of its parameters (except database type). You need to restart the Recorder before changes take effect.

To edit a database server:

1 Click **General Setup > Database Settings**, select a database, and then click **Edit**. Database settings for the selected database display.

2 Complete the fields as described in Creating a Database Server on page 80.

3 Click **Save**.

4 When prompted, restart the Recorder, as described in Starting and Stopping the Recorder and Components on page 59.

Deleting a Database Server

Delete a database server to remove it from the list of database servers for this Recorder. If this database server has dependent operations, a warning message displays asking for confirmation of the deletion. Deleting is not possible if you are trying to delete a media consolidator database and that is the only media consolidator in the system.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To delete a database server:

1. Click **General Setup > Database Settings**.
2. From the list of database servers, select an entry and click **Delete**.

   Note that the Delete button is disabled if only one database server is configured, as you cannot delete the only database.
3. Review any messages that display and click **OK**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring IP Recording Components

IP recording components include those components used in IP Recording and not in TDM (ITS IP) recording, with the exception of compression: compression is used in some TDM recording situations. All configuration is done from Recorder Manager.

Information is described in the following topics:

- Configuring Compression
- Managing Extensions

Configuring Compression

Configure compression to tell the Recorder which type of audio compression type (that is, codec) is to be used to compress inbound and outbound telephone calls. Compression compresses audio that is not originally compressed, meaning only uncompressed audio formats will undergo further compression.

When a voice signal is received on a telephone, it is in analog format. The codec converts the voice signal to digital audio format and compresses it at the same time. Compression provides efficient transmission to the destination. At the destination, the process is reversed, using the same compression type.

Compression is also used on some Cybertech voice cards. See Configuring Cybertech Voice Cards on page 142.

Recorder Manager allows you to set G723.1, G726, or no compression. You can also set mixed compression types for inbound and outbound calls. This information is presented in the following topic:

- Choosing Compression Options

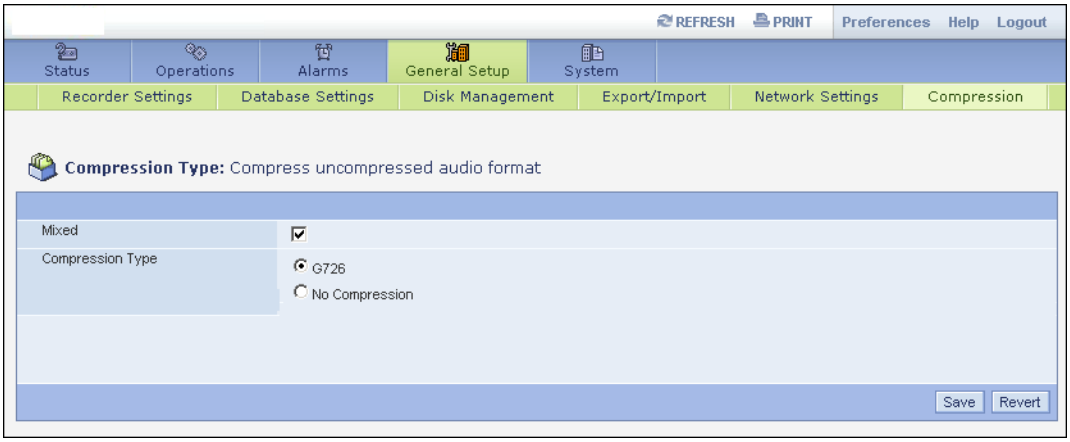
Choosing Compression Options

Choose an audio compression type to tell the Recorder which type of audio compression (that is, codec) is to be used to convert and compress G711 audio. Only if you have an IP Recorder installed, you can also choose the Mixed option. The recording of audio in the G.722 format is supported, however it cannot be replayed until it is transcoded into the G.711 or G.726 format.

To choose a compression type:

1 Choose **General Setup > Compression**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Choose a compression option according to the following:

Item	Description
Mixed (IP only)	Two one-way audio files are mixed into one two-way audio file, saving disk space. Mixing with G726 means that the input format whatever that is (with the exception of G.279) will be converted to G.726 and mixed.
G726	Choose this option to convert audio from the original format (with the exception of G729) to G726. G726 is a standard waveform codec used for compressing audio files.
No compression	No compression is used to compress audio files. No Compression converts G.722 to G.711

3 Click **Save**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Managing Extensions

Managing extensions describes the process of creating, editing, and deleting the telephone extensions in an IP recording telephony environment. If your Recorder is controlled by Enterprise Manager, all extension configuration is disabled and you need to refer to the *Enterprise Manager Administration Guide*.

You have two options for Recorder recording mode (Record and Do Not Record) and three options for extension record mode (Record, Application Controlled Recording, and Do not Record).

Telephones in IP recording, also known as SIP phones, support different protocols such as SCCP (Skinny Call Control Protocol, a Cisco proprietary protocol) and SIP (Session Initiated Protocol, an open standard). Extension recording modes are configured in Recorder Manager. They are configured in EM if your Recorder is managed by EM.

Note: If you are migrating from the previous software version and your Recorder is associated/managed by Enterprise Manager, all extension information is overwritten and maintained by Enterprise Manager, and you can ignore this section.

Information is presented in the following topics:

- Setting the Default Recorder Recording Mode
- Finding Extensions
- Creating Extensions
- Editing Extensions
- Deleting Extensions

Setting the Default Recorder Recording Mode

Choose one of two options to set as the Recorder’s default recording mode: record or not record. These options apply to extensions not in the list. The extension’s recording mode takes precedence when recording a call. It is the extension’s recording mode that determines if the call needs to be recorded. If the extension is not configured, then the Recorder's default recording mode, as listed beside Default Recording Mode, determines if the call needs to be recorded.

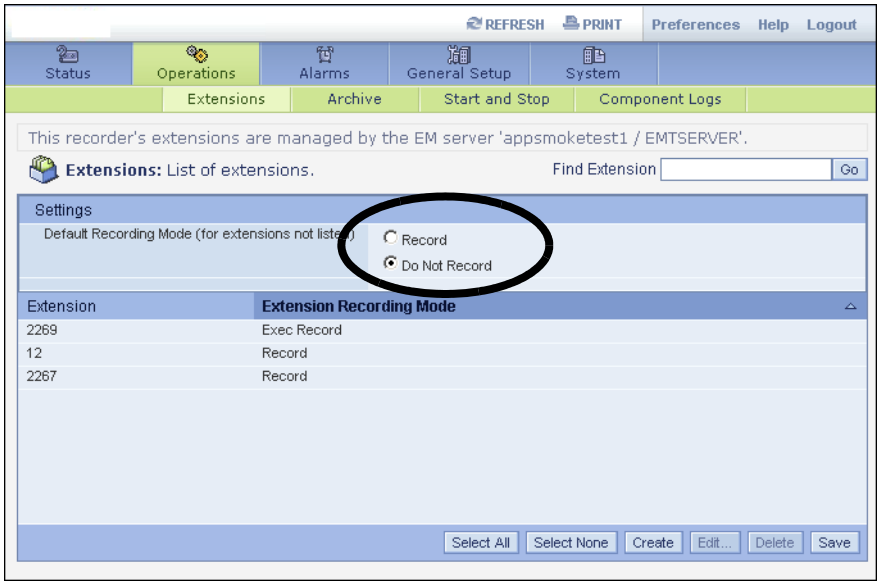
A cluster is a group of Recorders with the same extension recording configuration spread across the group. Clusters are created in Enterprise Manager. Clustered extensions can be edited and deleted only from Enterprise Manager.

See also Creating Extensions on page 88.

To set the recording mode:

1 In Recorder Manager choose **Operations > Extensions.** The extensions window displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Do one of the following:

- Select **Record** to set the default recording mode for all extensions NOT showing in the list to record calls. If an extension is configured/added to the list, the extension's recording mode will be used.
- Select **Do Not Record** to set the default recording mode for all extensions NOT showing in the list to not record calls.

3 Review settings according to the following table:

Recorder Recording Mode	Is Extension in List?	How will the call be recorded?
Record	Yes	Extension's recording mode will be used to determine if the call will be recorded (not the Recorder's recording mode).
Record	No	Call will be recorded.
Do Not Record	Yes	Extension's recording mode will be used to determine if the call will be recorded (not the Recorder's recording mode).
Do Not Record	No	Call will NOT be recorded.

4 Click **Save.**

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Finding Extensions

Use the Find Extension utility in the Extension window to locate an existing telephone extension. This is most useful where several pages of extensions exist and you wish to edit one or more extensions. You can also use it when only part of the extension number is known. In this utility, you can, in addition to searching, view each page of extensions by clicking the navigation arrows.

To find extensions:

1 Choose **Operations > Extensions.**

2 Do one of the following:

- In the **Find Extension** area, enter the extension to be found and click **GO**. The first occurrence of the found extension displays the page containing the extension and selects the extension. You can also enter the first few characters to search. If the Find operation fails, an appropriate message displays.
- In the **Page Navigation** area, which shows only if there are more than one page of extensions, click the up and down arrows to move between the pages of extensions.

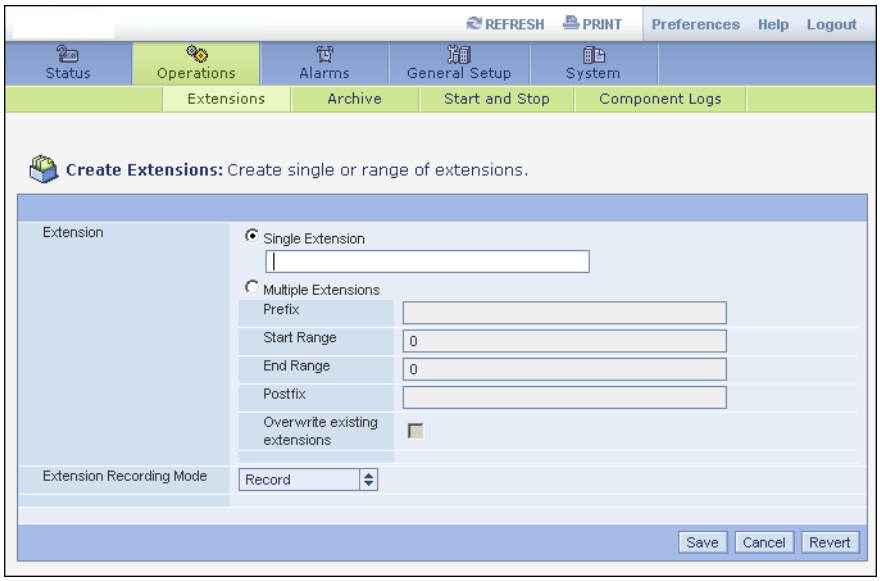
Creating Extensions

Quickly create one or multiple IP telephone extensions within your organization to be recorded according to a recording mode you assign. The telephone must be an IP phone. If you create one extension, you enter the extension, assign a recording mode and save. Creating multiple extensions is a simple process also: you enter a start and end range for the extension numbers (maximum 10,000 per Recorder) and then assign an extension recording mode. The recording mode then applies to the whole range of newly-created extensions.

To create extensions:

1 In Recorder Manager choose **Operations > Extensions,** and then click **Create**. The Create Extensions window displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Do one of the following:

- Click **Single Extension** to create one extension and then enter enter an extension number such as 3355. Numbers can be all numeric or alpha-numeric.
- Click **Multiple Extensions** and complete the following fields:

Item	Description	Required?
Prefix	Numbers or letters that precede the extension number such as AB. Extension 3455 would be AB3455.	Optional
Start Range	The beginning numeric value of the extension range, such as 3455. Remember that you cannot create more than 10,000 extensions on a single Recorder.	Required
End Range	The ending numeric value of the extension range. Remember that you cannot create more than 10,000 extensions on a single Recorder.	Required
Postfix	Numbers or letters that appear at the end of the extension number (also known as a suffix).	Optional
Overwrite existing extensions	Checkbox used only for Multiple Extension creation that determines if pre-existing extensions with the same number will be overwritten (if checked). Unchecked by default.	N/A
Note: All extensions must be named according to the SIP URI naming convention as described in section 19.1 or SIP RFC 3261.		

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 Choose as an **Extension Recording Mode** one of the following: Record, Do not Record, Application Controlled, as in the following table:

Item	Description
Record	See Setting the Default Recorder Recording Mode on page 86
Do not Record	See Setting the Default Recorder Recording Mode on page 86
Application Controlled	See Editing Extensions on page 90

For example, in EM, while creating or assigning extensions to an IP extension pool, you can have any one of the following recording modes: **Record, Do Not Record, Application Controlled,** and **Start of Business Rule**. Since **Start of Business Rule** is specific to the Integration Service, whenever you associate this IP extension pool to a Recorder, these extensions are pushed (sent automatically) to the Recorder. In RM, the **Start of Business Rule** mode does not exist, therefore whenever you create extensions in EM with mode Start of Business Rule and they are pushed it to the Recorder, RM shows the mode as Application Controlled, resulting in the following mapping:

Item	Mapping in RM
EM	RM
Recorder	Record
Do Not Record	Do Not Record
Application Controlled	Application Controlled
Start of Business Rule (EM Only)	Application Controlled.

4 Click **Save**.

Editing Extensions

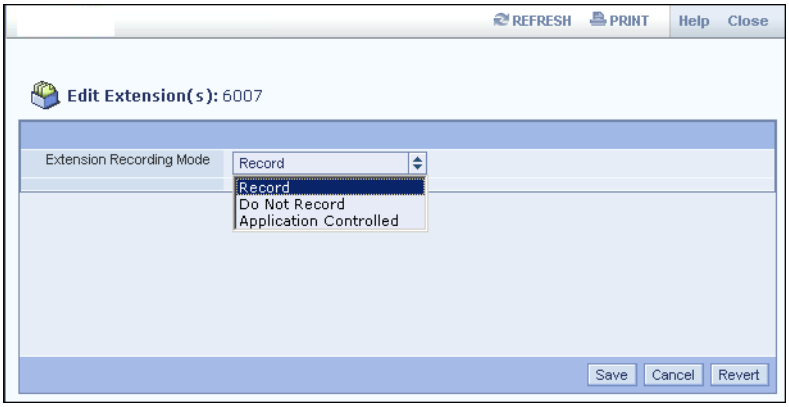
Edit IP extensions to assign a different Extension Recording Mode (Record, Application Controlled Recording, and Do Not Record) to one or to multiple IP telephone extensions. The recording mode then applies to all selected extensions.

To edit extensions:

1 Choose **Operations > Extensions,** and then select one or more extensions.

2 Click **Edit**. The Edit Extension window displays. If you selected only one extension, the extension number shows, such as 5499. If you selected more than one extension, the text Multiple Extensions Selected displays beside Edit Extension(s).

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



3 In the **Extension Recording Mode** field, choose a recording mode according to the following:

Extension Recording Mode	Description
Record	The Recorder records all call segments of the displayed extension(s) whenever the extension(s) are in use, according to the recording settings for the Recorder. **Note**: A call segment is the period from start of conversation to either call end, call hold or transfer of the call from the specified device.
Application Controlled Recording	The Recorder records all call segments of the displayed extension(s) whenever the extension(s) are in use, according to requests from an application such as Enterprise Manager, ExecRecord and Live Monitor. With **ExecRecord**, All records of the calls are retained by the Recorder during the call. The recordings are deleted when the call is over, unless you press the record button (the ExecRecord button) on the phone. **Live Monitor** is similar to the ExecRecord mode. Calls are retained by the Recorder during the call and are deleted at the end of the call, unless you click the **Record** button in the Observer application, assuming that Live Monitor is set up for this extension.
Do not Record	No calls are recorded, regardless of default recording mode.

4 Click **Save**.

Deleting Extensions

Delete extensions to remove them from the extensions list. For example, instead of editing an extension number, it might be easier to delete and create a new one. You cannot delete extensions that are grouped in a cluster.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To delete extensions:

1 Choose **Operations > Extensions,** and then select one or more extensions.

2 Click **Delete**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Optional Components

Configuring optional components describes how to configure Live Monitor, Screen Recording, and Archive. For other components and applications that can be optionally added to the Recorder system, refer to the Documentation folder on the installation CD.

Information is described in the following topics:

- Configuring Live Monitor and Observer
- Configuring Screen Recording
- Configuring Centralized Archiving

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Live Monitor and Observer

Configure the Live Monitor option, which allows supervisors to *listen in* to calls between agents and customers, to designate a Recorder server that will act as the Live Monitor Server host, and to provide connection settings and metadata mapping information. Connection settings connect the Live Monitor Server to Capture Engine processes in each Recorder, facilitating Live Monitor functionality throughout the organization.

The Live Monitoring of encrypted audio is not supported. The G722 audio format is supported by Live Monitor.

Configuring Live Monitor is described in the following topics:

- Understanding Live Monitor
- Defining the Live Monitor Server
- Defining Observer Column Mapping
- Configuring Observer
- Creating Live Monitor Attributes
- Editing Live Monitor Attributes
- Managing Live Monitor Attributes
- Adding and Deleting Attribute Tags
- Setting Restrictions for Live Monitor Replay
- Re-arranging the order of Columns
- Troubleshooting Live Monitor

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Understanding Live Monitor

You can view any call currently being recorded, provided you have the replay permission. This is accomplished through Live Monitor's Live State component and the Observer application. The Live State component is built into every Recorder's software architecture. This component does three things:

- Tracks every call currently being recorded,
- Receives replay requests from Observer
- Verifies with the eWare database if the Observer user's login credentials permit the replay of calls from specified extensions.

At the same time, Observer performs parallel tasks:

- Communicates continuously with the Live State component,
- Lists all eligible (for monitoring) calls currently being recorded (based on replay restrictions as described in Setting Restrictions for Live Monitor Replay on page 104),
- Optionally displays calls in user-defined columns, as described in Defining Observer Column Mapping on page 97.

Once the Recorder is designated as a Live Monitor server, which enables the Live Monitoring process, all eligible (for monitoring) calls being recorded display in Observer. This allows a supervisor or other authorized user with replay rights to select a call of interest, and then click the Play button in Observer to play the call.

An optional AudioServer component is also available. This component has its own software that allows calls to be replayed over a telephone. Audio server is used in conjunction with Web Observer, and not the regular Observer, to list eligible (for monitoring) calls.

You should plan for additional channels if you are using Live Monitor. In sizing for Live Monitor, you estimate the number of channels required to allow for concurrent call recording and Live Monitoring.

To estimate the number of channels including Live Monitor:

1. Determine the number of Live Monitor/Observer connections in the organization.
2. Find out how many channels are available for call recording.
3. Allow for one additional channel for every 5 concurrent Observer connections. For example, a 100 channel Recorder with a Live Monitor server expecting 100 concurrent Observer connections would be sized as a 120 channel Recorder.

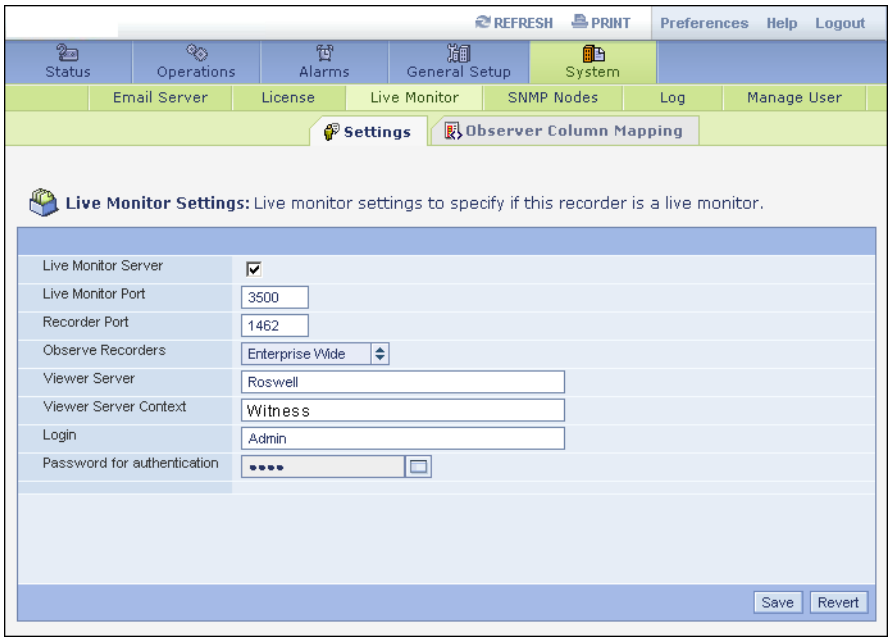
Defining the Live Monitor Server

Define the Live Monitor server to assign the current Recorder server as Live Monitor server host and to set connection details. Live Monitor settings are also required to configure Observer.

To define the Live Monitor server:

1. In Recorder Manager click **System > Live Monitor > Settings**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Complete the settings screen as follows:

Field	Description
Live Monitor Server	Click to place a checkmark to indicate that this Recorder server will be used as a host for the Live Monitor server. Until you check this field, all other fields will be disabled. **Note**: In some cases there may be too many channels and performance will be affected by Live Monitor. For example, the live streaming requirements of call replay might slow the processor on the PC. In that case, installing Live Monitor on a less busy server or even on a server by itself is recommended. For Live Monitor architecture topography scenarios, refer to the *System Infrastructure Guide.*
Live Monitor Port	Accept the default port 3500 or type the correct port number. This is port on the Recorder server through which Live Monitor *listens* to (that is, communicates with) the capture components on all Recorders being monitored. If your network or firewall software blocks the default port, use an alternative port. For a list of ports used by the Recorder, refer to *Recorder Installation Guide.*
Recorder Port	Accept the default port 1462 or type the correct port number. This is the port on the host Recorder server through which Live Monitor connects to the capture component on the host Recorder.
Observe Recorders	Select **By Location** or **Enterprise Wide** to direct Live Monitor to provide service to (that is, to *observe*) Recorders at locations you specify, or to all Recorders in the organization respectively.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Viewer Server	Type the name of the Search and Replay (Viewer) server that controls the current installation of Live Monitor. It is through this Search and Replay server that call replay rights and restrictions are set.
Viewer Server Context	Type one of the following values exactly, depending on the brand of Viewer being used: **Witness, Nortel, Avaya.**
Login	Type the login Username (no spaces) for the Search and Replay administrator.
Password for Authentication	Type the Password for the Search and Replay administrator.

3 Click **Save**.

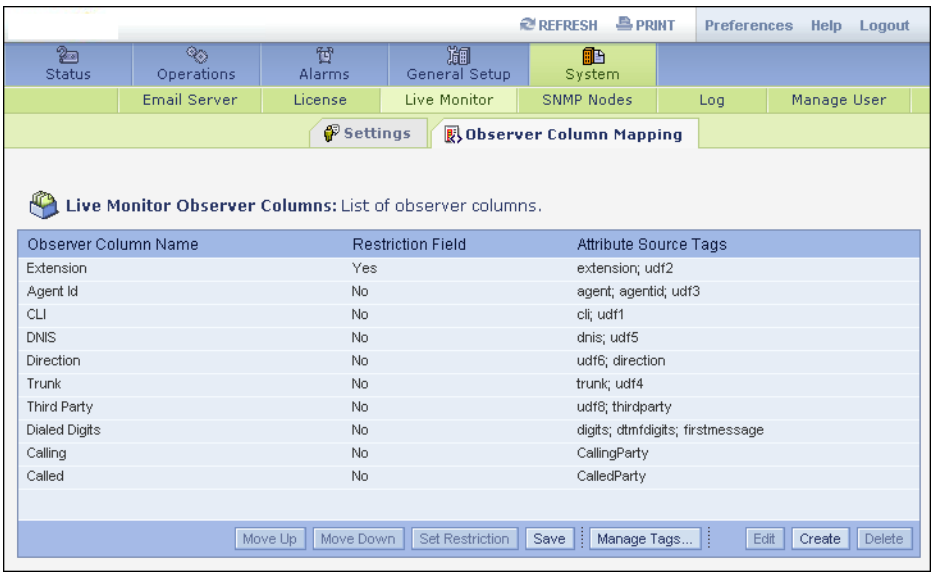
Defining Observer Column Mapping

Define Observer Column Mapping to assign names to the default attributes tags provided to the Recorder, so that you can view more details while Live Monitoring calls. In this window you can edit, create, manage, and delete tags as well as rearrange rows and indicate replay restrictions.

The Restriction field must always be in column one (the top row) for Observer to display calls correctly. Use the Move Up feature to ensure that the Restriction field is always in column one.

To define live monitor column (attributes) tags:

1 Click **System > Live Monitor > Observer Column Mapping**.



© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

2 Review Observer Column Mappings according to the following:

Field	Description
Observer Column Name	Shows the names of columns (attributes) as they will appear in Observer.
Restriction Field	Shows whether the attribute has any replay restrictions attached. Only one field can be a restriction field. For example, supervisors are restricted to monitoring only certain extensions. The Extension field, therefore, would have restrictions. Restrictions are configured separately in Search and Replay.
Attribute Source Tags	Shows a listing of the source tags, derived from a Unify script or other Data Source, that correspond to the Observer Column Name

3 Do one of the following:

- Click **Move Up** or **Move Down** with row selected to move that row up or down.
- Click **Set Restriction** with the Extension row selected, if necessary, as described in To set restrictions for Live Monitor replay: on page 104.
- Click **Manage Tags** to open the Tag Management window as described in To manage Live Monitor attributes: on page 103. You can also access the same Manage Tags feature from the Edit and Create windows.
- Click **Edit** with a row selected to edit an attribute as described in To edit a Live Monitor attribute: on page 102.
- Click **Create** to create an Observer column name and assign tags, as described in attribute as described in To edit a Live Monitor attribute: on page 102.
- Click Delete to delete a row (that is, an Observer column) as described in To delete an attribute tag: on page 104.

4 Click **Save**.

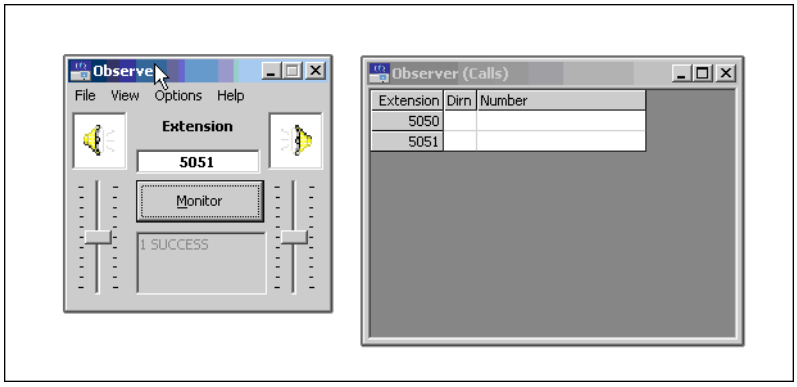
Configuring Observer

Configure Observer to identify the IP address and Port number of Unify so that Observer can live monitor calls. Make sure the Recorder PC has a sound card installed or extension(s) configured so that Observer can operate properly. Observer does not start if a sound card or extensions are not present.

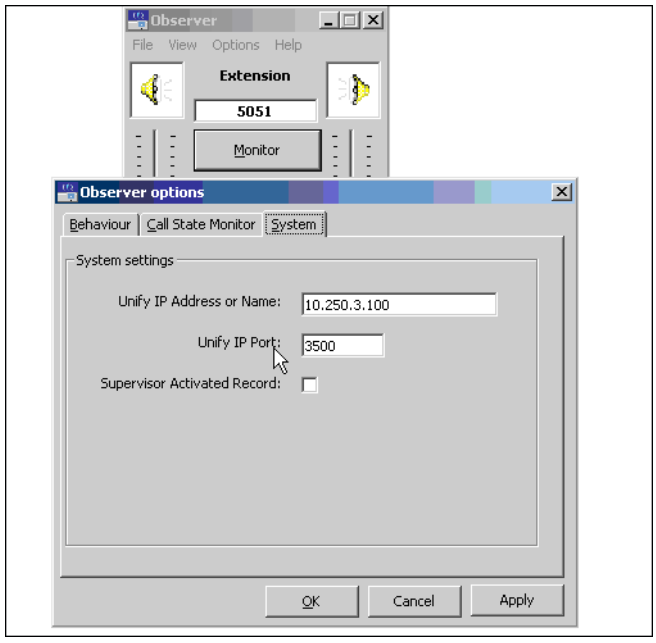
To configure Observer:

1 On the desktop of your Recorder PC, click **Observer**. The Observer window displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



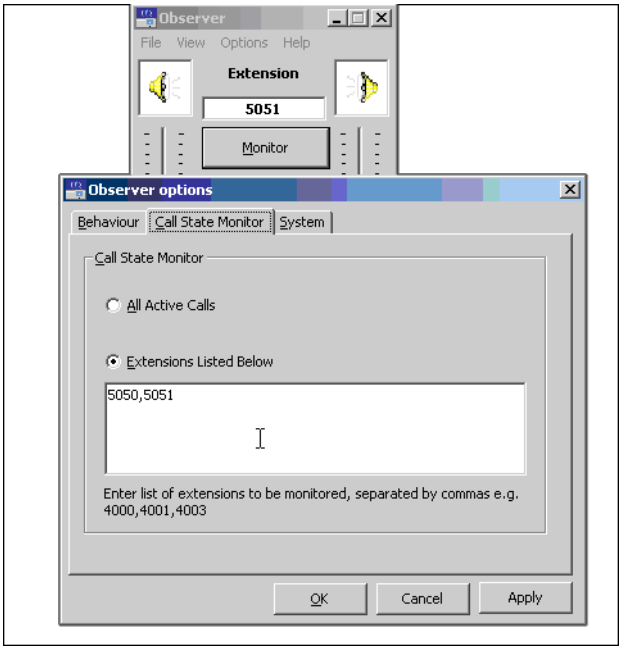
2 Click **Observer > Options**, and then click **Systems**.



3 Verify that the **Unify IP Address or Name** field contains the address or name of the Recorder server, and that the **Unify IP Port** field shows the same port number as the Live Monitor Port set as described in Defining the Live Monitor Server on page 95.

4 Click **Options > Call State Monitor**. The Call State Monitor window displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



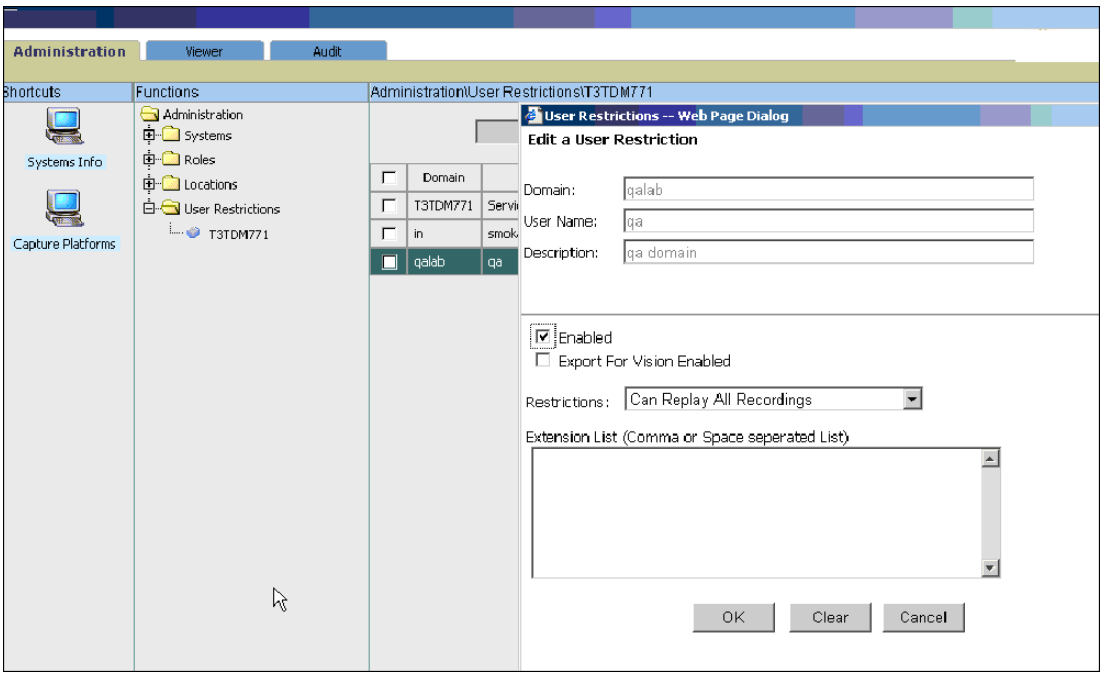
5 Select either **All Active Call** or **Extensions Listed Below**. If you select **Extensions Listed Below**, specify the extensions to be monitored, and then click **Apply** or **OK**.

6 Click **Observer**, and then click the **Monitor** button. The extensions to be live monitored are now set up.

7 Verify the setup in Viewer by following these steps:

- Launch Viewer and click **Administration > User Restrictions**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



- Click **Add** to add user restrictions to monitor the calls.
- Click **Enabled** and provide the restrictions according to business needs.

8 Click **OK** to save. Now, only the User who can replay the calls is able to monitor the calls.

Creating Live Monitor Attributes

Create live monitor attributes (columns) to add a new column name and assign one or more tags from the list of available tags to Observer Column Names.

To create a live monitor attribute:

1 In Recorder Manager, click **System > Live Monitor > Observer Column Mappings > Create**. The Create Attribute window displays.

2 In the **Observer Column Name** field, type a unique name for the column as it will appear in the Observer application.

3 Complete the Tags section as described in To edit a Live Monitor attribute: on page 102.

4 Click **Save**.

Editing Live Monitor Attributes

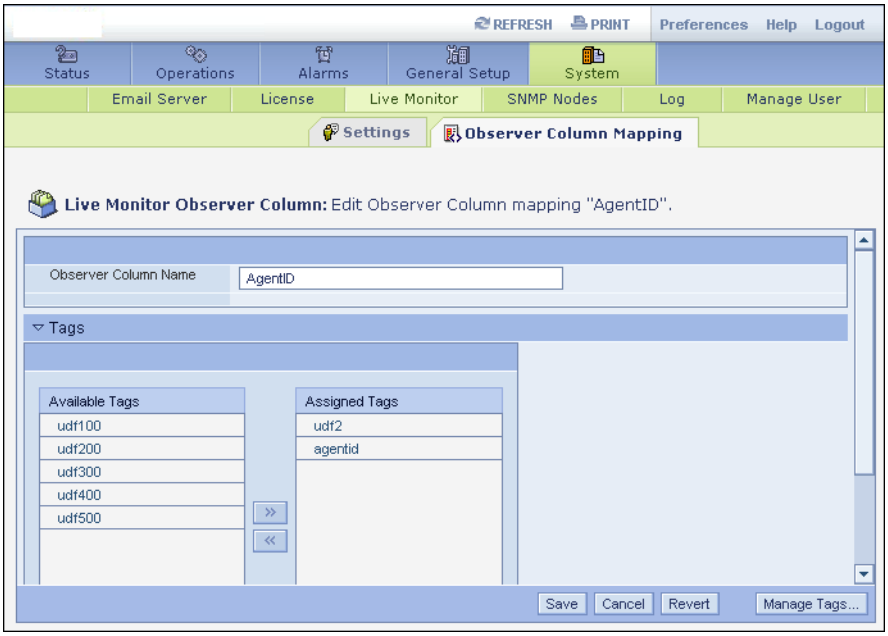
Edit Live Monitor attributes to assign one or more tags from the pool of available tags to Observer Column Names.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To edit a Live Monitor attribute:

1 Click **System > Live Monitor > Observer Column Mappings**.

2 Select any row, and then click **Edit**. The Edit Tag window displays, showing available tags and tags already assigned to the selected column.



3 Select one or more rows in the **Available Tags** pane, and then click the right arrow button to move the selection to the Assigned Tags pane.

Press the Ctrl key and click two or more rows to make a multiple selection.

4 Remove items in the **Assigned Tags** pane by selecting items and clicking the left arrow button.

5 Do one of the following:

- Click **Save** if you are finished reassigning tags.
- Click **Manage Tags** to add, edit, or delete tags, as described in Managing Live Monitor Attributes on page 102.

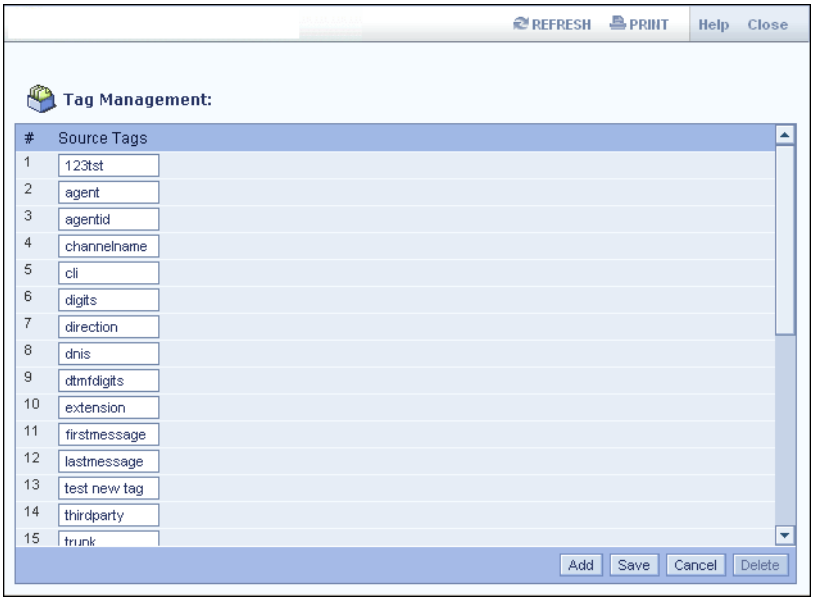
Managing Live Monitor Attributes

Manage Live Monitor attribute tags to rename existing columns that may have an obscure or misspelled name and to add and delete tags. For example, instead of a column named **`UDF 22`** you could type an identifiable name such as **`Dialed Digits`**. This makes Live Monitor and Observer easier to use.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To manage Live Monitor attributes:

1 In the Observer Column Mapping window click **Manage Tags** or follow the steps described in Editing Live Monitor Attributes on page 101 and choose **Manage Tags**. The Tag Management window displays.



2 Select any displayed name and type a new name.

To rearrange the order of the tags, refer to Re-arranging the order of Columns on page 104.

3 Do one of the following:

- Click **Add** to add a new tag as described in Adding and Deleting Attribute Tags on page 103.
- Click **Save** if you are finished editing tags.
- Select one or more tags and click **Delete** to delete those tags, as described in Adding and Deleting Attribute Tags on page 103.

Adding and Deleting Attribute Tags

Add and remove any source tags as necessary by using the Manage Tags button in the Tag Management window. The default configuration supplied with the system contains the available call information tags typically used, but sometimes you may have to add tags not present or remove tags not being used. This would be done if the Unify Script at the customer site was customized to use different tag values than the default Recorder values.

To add a new attribute tag:

1 Click **System > Live Monitor > Observer Column Mapping.**

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

2 Select the column to which the new tag will be added and click **Edit**. The Observer Column Details window displays.

3 Click **Manage Tags**. The Tag Management window displays.

4 Click **Add** and type a name for the new tag.

5 Click **Save**.

To delete an attribute tag:

1 Click **System > Live Monitor > Observer Column Mapping**.

2 Select the row containing the tag to be deleted, click **Edit,** and then click **Manage Tags**.

3 Select the tag to be deleted, and then click **Delete**.

Setting Restrictions for Live Monitor Replay

Set restrictions to identify which tags being live monitored have a replay restriction. The Set Restriction operation does not create the restriction - the restriction is created in Viewer, as described in the *Viewer User Guide.* Set Restriction only indicates that the field is subject to replay restrictions. For example, most supervisors are restricted to monitoring only certain agent extensions. The Extension field, therefore, would have restrictions that specified those extensions that could be live monitored or which extensions were to be excluded.

To set restrictions for Live Monitor replay:

1 Click **System > Live Monitor > Observer Column Mapping.**

2 Select **Extension**, and then click **Set Restriction**. The value in the Restriction Field cell toggles between **Yes** and **No**.

Yes indicates that the field is subject to live monitor replay restrictions, and No indicates not. Replay restrictions are created in Viewer.

3 Click **Save**.

Re-arranging the order of Columns

Re-arrange the order of columns to improve the display of column information in the Observer application, thereby improving Live Monitor functionality.

To rearrange the order of columns:

1 Click **System > Live Monitor > Observer Column Mapping**. See also Defining Observer Column Mapping on page 97

2 Review the names in the rows under **Observer Column Name** and rearrange rows by selecting any row and clicking **Move Up** or **Move Down**.

3 Click **Save** when the rows are in the desired order.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Troubleshooting Live Monitor

Problem	Likely Solution
Cannot use Observer (with an older Recorder) to live monitor calls	Change the domain name in Viewer (Search and Replay) from <domain>.com to <domain>.
Rows keep being added and removed from the Calls window.	This is normal. The Call Status Monitor window shows only calls in progress. When a call ends, the row is removed from the Calls window.
Sometimes, if left running, Live Monitor playback stops unexpectedly.	Live Monitor encounters a trunk-side channel that has not been configured to be monitored.
If Live Monitor is left running, it plays back only calls on one extension.	This is normal for trunk-side or station-side recording, because the channel is fixed to the extension. To resolve, choose another extension to monitor.
The Volume slider on the right does nothing.	This slider is used for recording stereo calls in IP environments to allow you to control volume separately for each side.
Cannot connect to the Viewer Server	Check that the Search and Replay Server name is correct and is running. Check also to make sure that the username and password are correct.

Configuring Screen Recording

Configure optional screen recording functionality in the Recorder, providing you have the necessary licenses, to enable the capture of an agent's workstation screen activities and metadata relating to a call. Any screen information, except for Live Monitor (screen Live Monitor on demand is not supported), is captured and stored in a content file (with a .scn extension) while the metadata is similarly persisted as a .xml file. Thereafter, information is searched for and retrieved as with recorded calls, a process formerly completed by the Funk screen capture engine.

This information is described in the following topics:

- Enabling the Screen License
- Configuring Unify or IS to Record Screens
- Setting Channels to be Recorded

Enabling the Screen License

Enable the screen license for screen recording to show the number of channels that are licensed, by indicating channel allocation for audio and screen recording. Channels

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

assigned for either type of recording cannot be used by the other. For example, if the concurrent Recording Limit is set to 100, and screen and audio recording are both enabled, 50 channels are assigned for screen recording, and 50 channels are assigned for audio (that is, calls). Once the 50 channels of screen are being recorded, unused audio channels cannot be used for a 51st screen recording. Only a maximum of 50 concurrent screen recording can take place.

You can enable screen licensing when applying for a new license or when updating an existing license by clicking Enable Screen Recording, as described in Configuring the Recorder License on page 23.

Configuring Unify or IS to Record Screens

Configure Unify to record screens if you do not have the Integration Service (IS) installed on your system. Unify is common in single-box solutions or in legacy systems, and requires detailed scripting as well as configuration of the Unify server by using Unify's CTI Studio software application. For more information, refer to the *System Infrastructure Guide*. You can also configure screen recording from the IS by using Enterprise Manager. This is the preferred method, requiring that the IS be installed. No external configuration is required. For more information, refer to *Setting up for Screen Recording* in the *Enterprise Manager Administration Guide*.

Setting Channels to be Recorded

Set the number of channels to be recorded to show the maximum number of concurrent channels available for screen recording, as determined by your license. To do this, type in the Screen Recorder settings described in Configuring Recorder Settings (Call Buffer) on page 62.

Configuring Centralized Archiving

Configure the optional Centralized Archiving (formerly known as CAM and Enterprise Archive) to set up archiving activities that are additional to the local archive capabilities of the Recorder. Centralized Archiving drives are configured in Recorder Manager. However, media and campagin configuration is done outside Recorder Manager by the Centralized Archiving administration application. Information is presented in the following topics:

- Configuring Centralized Archiving Drives
- Configuring Centralized Archiving Settings
- Troubleshooting Archive

For more information on using centralized archiving, refer to the *Centralized Archiving Installation and Administration Guide* found in the Centralized Archiving Installation CD/DVD.

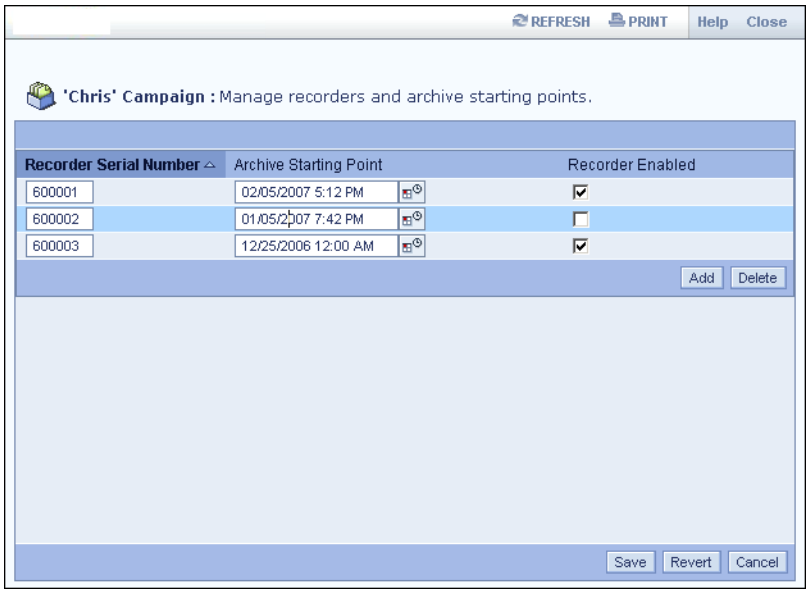
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Centralized Archiving Drives

Configure drives to be used with Centralized Archiving from the Content Source area of the Archive window in Recorder Manager, as described in Configuring an Archive Drive on page 67. In the **Content Source** area, choose **Centralized content from Campaign** to indicate that the drive is used as a Centralized Archiving drive and then type the name of the campaign. When Archive is installed, the Manage Campaign Recorders button is enabled, allowing you to add or remove Recorders from the campaign.

To manage campaign Recorders:

1 Follow the steps described in Configuring an Archive Drive on page 67, and then click **Manage Campaign Recorders.**



2 Complete the fields in the Manage Campaign Recorders screen as follows:

Item	Description
Recorder Serial Number	Type the serial number of the Recorder to be added to the Campaign.
Archive Starting Point	Click the icon and choose a date and time, as described in Configuring an Archive Drive on page 67.
Recorder Enabled	Check to enable the Recorder to record contacts (calls and screens) in the current campaign.

3 Click **Add** to add another Recorder to the campaign, or click **Delete** to remove a Recorder from the display.

4 Click **Save** to save the settings.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

For all other Centralized Archive administration, refer to the Administration pages of the Centralized Archive application, which is installed from a separate installation CD.

Configuring Centralized Archiving Settings

Configure settings for Centralized Archive to archive contacts recorded from multiple Recorders to a single location. Usually, this means that a subset of all recorded contacts are to be archived. Centralized Archive is installed as a separate application either on a standalone server with its own database, or on an existing Recorder server.

To configure Centralized Archiving settings:

1. Launch the Admin application for Centralized Archiving and open the archive query template.
2. Use the archive query template to create a **Campaign** and a **Rule**.

   For environments that have other types of Recorders, you must create a **Composite Query Template** to create the rule. For more information, refer to the *Centralized Archiving Installation and Administration Guide.*
3. Follow procedures described in the documentation that accompanies your Centralized Archiving software.

Troubleshooting Archive

If you experience problems with archive drives, make sure that the following are true:

- The Recorder platform type **Full-time Recorder** has been created in the working database.
- The archive view and query template for the Recorder is created.
- At least one archive storage device has been created.
- The Archive Admin application has been installed properly.
- The working database is up and running.
- The Recorder is up and running.
- The Recorder Call Buffer has been configured and there are contacts in the buffer.
- The Call Buffer on the Recorder is created as a Storage Device in the media database.
- The Call Buffer Storage Device in the media database is associated to the capture platform for the Recorder.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Chapter 3

Using Voice Cards, NICs and Analyzer

Using Voice Cards, NICs, and Analyzer describes how to configure TDM (ITS IP Recorder) and IP Recorder devices. This includes how to configure voice cards for the TMD Recorder (ITS IP Recorder) installation of the Recorder, Network Interface Cards (NICs) for the IP Recorder installation of the Recorder, and the optional Remote Analyzer IP call control device.

Voice cards and NICs are industry standard CTI interface cards that are inserted into a slot in the chassis of the Recorder PC. Voice cards capture the audio portion of calls in a TDM environment and propagate data to the Workflow component for further processing. NICs direct the flow of data in an IP environment by connecting to the data network.

Note: TDM Recorder (ITS IP Recorder) refers to a Recorder that uses traditional TDM or IP emulation on channels. IP emulation uses the same channels as TDM only with a layering protocol that emulates IP, known as pseudowire emulation (PWE3).

Analyzer is included as a CTI capture device, as this optional device, which is located in a server on its own, controls and distributes call control data in an IP environment from an IP switch to data packet capture devices. The Analyzer is managed by Analyzer Manager, which is a software application similar to Recorder Manager. For more information, refer to the *System Infrastructure Guide*. This information is described in the following topics:

- Configuring Voice Cards
- Configuring Network Interface Cards
- Configuring Analyzer

Configuring Voice Cards

Configuring voice cards in a TDM recording environment describes general voice card tasks such as viewing and identifying the various cards, as well as specific information on each card type supported. Information is presented as properties and channels for digital and analog voice cards. Only T1/E1 cards record trunk-side (that is, between the switch and PBX). All other cards record station-side (that is, between the PBX and extensions), so that trunk settings apply only to T1/E1 cards.

The Recorder license must be updated from the Recorder license screen to perform any operation on the voice cards. If not, the voice cards do not display in the configuration screen.

Information is described in the following topics:

- Performing General Voice Card Tasks
- Configuring T1/E1 Voice Cards
- Modifying the Trunk Protocol on a T1 Voice Card
- Modifying the Trunk Protocol on a E1 Voice Card
- Configuring PCM32 Voice Cards
- Configuring NGX Voice Cards
- Configuring Cybertech Voice Cards
- Configuring Analog Voice Cards
- Voice Card Troubleshooting

For additional information on voice cards, refer to the Ai-Logix SmartWorks and Cybertech guides in the documentation folder on the Recorder install CD/DVD.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Performing General Voice Card Tasks

Perform general voice card tasks using Recorder Manager to view, add and modify settings on an existing or replaced card. Compatible voice cards appear in Compatible Voice Cards on page 242. Information is described in the following topics:

- Viewing Voice Cards
- Copying the Configuration of a Voice Card
- Identifying a Voice Card
- Deleting a Voice Card
- Adding a New Voice Card
- Replacing a Voice Card
- Modifying the Properties of an Existing Voice Card
- Viewing Voice Card Channels
- Updating the Configuration of Voice Card Channels
- Editing Tags for Voice Card Channels

Viewing Voice Cards

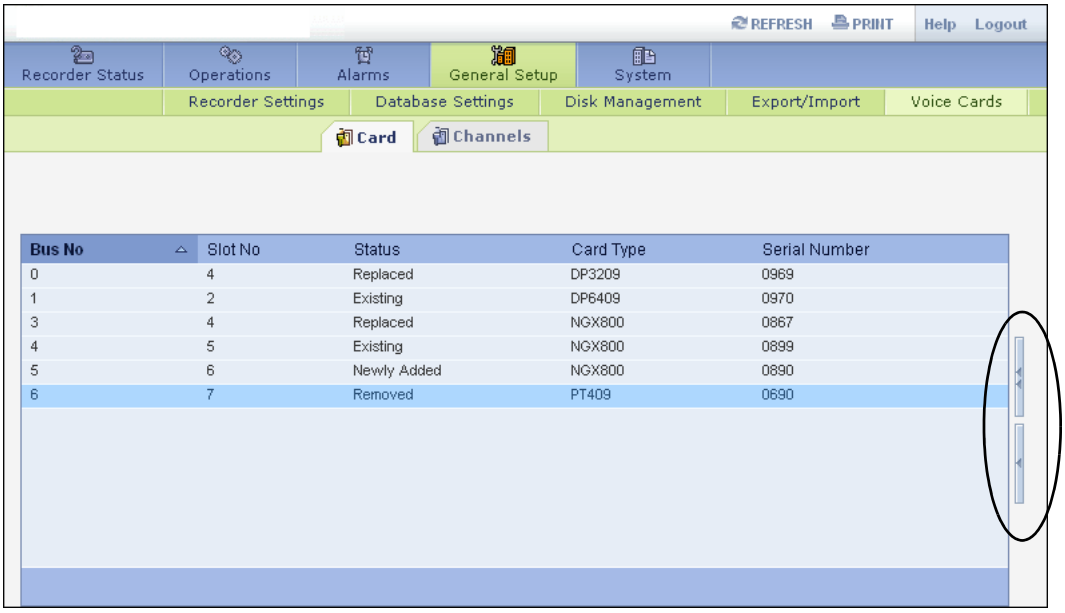
View voice cards to view a list of all voice cards in the Recorder, take action on one or more cards, and find out where in the computer the voice card is located. Details of any selected card (in the left pane) show in the right pane.

During the initilization of the Recorder, if there are any faulty Ai-logix cards then an alarm is triggered and an alarm message displays. After this message displays you may disable and replace the card, or ignore the message. If you ignore the message, the Recorder skips the faulty card and proceeds with the initialization of the other cards.

To view voice cards:

1 Choose **General Setup > Voice Cards** > **Card**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Click the toggler arrow between the two panes (circled) to maximize the card details window, and then review information according to the following:

Field	Description
Bus No.	Shows a read-only number of the data bus on which the card is located in the PC.
Slot No	Shows a read-only number of the slot on the computer's motherboard on which the card is located.
Status	Shows the status of the card as one of either Existing, Replaced, Newly Added, and Removed. • **Existing** is a previously existing card that can be reconfigured. • **Replaced** is a card that has taken the position of an Existing card and may or may not require configuration. • **Newly Added** is a new voice card that is physically located in the PC but awaits configuration. • **Removed** refers to an empty slot representing a card that was removed from the PC. **Note**: The configuration of the card remains in the configuration xml file.
Card Type	Shows the model number and type of the card, as described in Compatible Voice Cards on page 242.
Serial Number	Shows the unique serial number of the voice card. The Capture engine uses this serial number in generating a recording's audio file and .xml files. For example, a metadata file from call number seven captured on a voice card with serial number 600001 would be **`600001000000000.xml`**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 When finished, click the left pointing arrow on the right side of the window to expose the voice card details window.

Copying the Configuration of a Voice Card

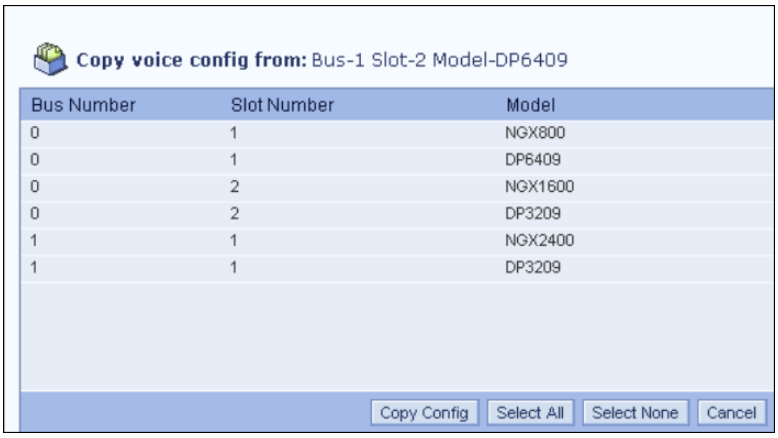
Copy the configuration of a voice card with a status of Existing to one or more other voice cards of the same type, regardless of their status. The card's model number and all pertinent configuration information is copied. Bus numbers and slot numbers are not copied.

To copy the configuration of a voice card:

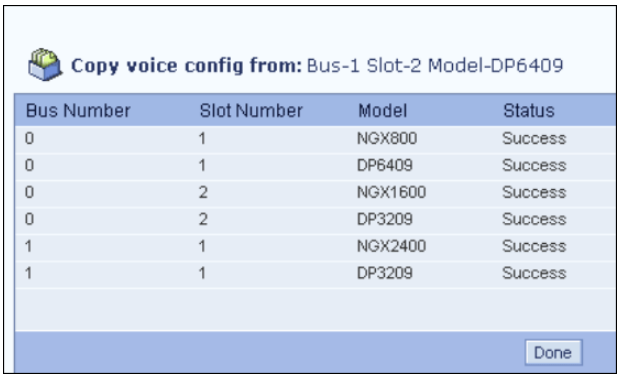
1 Choose **General Setup > Voice Cards** > **Card**.

2 In the List box (left pane) select a voice card with a status of **Existing** or **Removed.**

3 Click **Copy Card.** A list of installed voice cards displays.



4 Select one or more cards, and then click **Copy Config**.



© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

5 Select one or more cards to copy to, and then select **Copy**. The voice card configuration is copied from the source to the destination.

You can copy cards only of the same family. For example, if you select an NGX card as the source, the destination cards allowed for copy are only of type NGX.

Results of the copy display, showing the status for each voice card that is being copied to.

6 Click **Operations > Start and Stop** and reboot if requested.

Identifying a Voice Card

Identify a voice card by selecting the card in the Recorder Manager and clicking Identify. A light blinks on the back of the hardware, indicating where the card is physically located. You can have as many cards as there are available card slots on the PC (typically maximum 15), so that when you click the Identify button, the light on the corresponding card displays.

To identify a voice card:

1 Choose **General Setup > Voice Cards > Card** and select a card.

The **Identify** function works for all card statuses except Removed.

2 Click **Identify**. A light blinks on the card (on the back of the hardware). If the light does not appear, check connections (card seating and wire connectors) and retest. If the light still does not appear, the card may be defective and require replacing.

Some card lights cannot be seen from the back of the PC or from the server as they appear only on the voice card.

Deleting a Voice Card

Delete a voice card to remove a selected card from the configuration window. All cards, regardless of status, are eligible for deletion. For example, a voice card may be removed from one Recorder and relocated in a different Recorder.

To delete a voice card

1 Choose **General Setup > Voice Cards > Card**.

2 In the List box (left pane) select a voice card, regardless of status.

3 Click **Delete**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Adding a New Voice Card

Add a new voice card to install and configure a new compatible voice card into a Recorder.

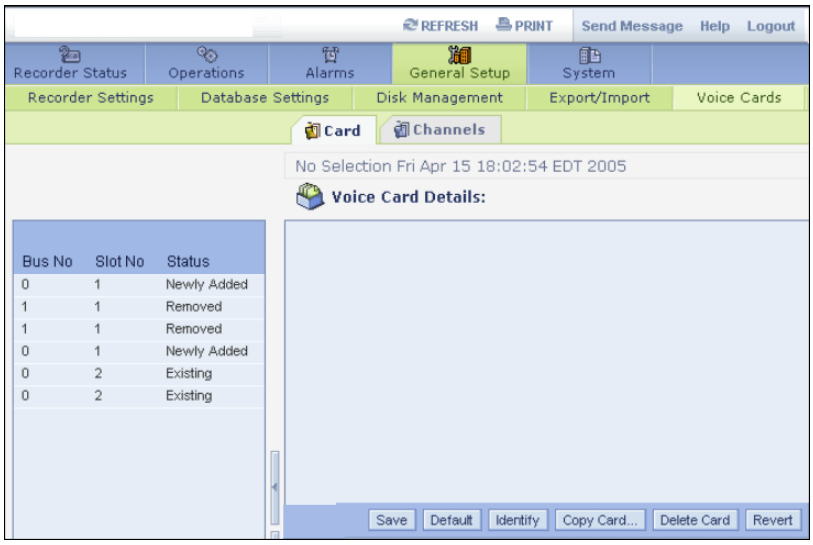
To add a new voice card:

1. Insert a compatible voice card (see Compatible Voice Cards on page 242) into an empty slot on the bus of the Recorder PC.

   Caution: Extreme care should be taken when inserting voice cards or any other component into a PC. Tools with magnetic tips should be used with extreme caution. Wearing an anti-static cuff is strongly recommended to prevent static electricity.

2. Click **Operations > Start and Stop** and choose **Reboot** to reboot the system. The Recorder detects and displays the new card's slot number, serial number, and other metadata.

3. In the Recorder Manager click **General Setup > Voice Cards > Card.** The card you added appears in the left pane with a status of **Newly Added**.



4. Configure the voice card as necessary or leave all settings at their defaults and click **Save**.

   If an unsupported card (such as a card other than Ai-Logix) is detected, its factory default information may display. However the card cannot be configured and you should replace the unsupported card with a supported one.

5. Click **Channels** to review channels available, as described in Updating the Configuration of Voice Card Channels on page 118.

6. Click **Save**. The status of the voice card changes from **Newly Added** to **Existing.**

7. If prompted, restart services by choosing **Operations > Start and Stop**.

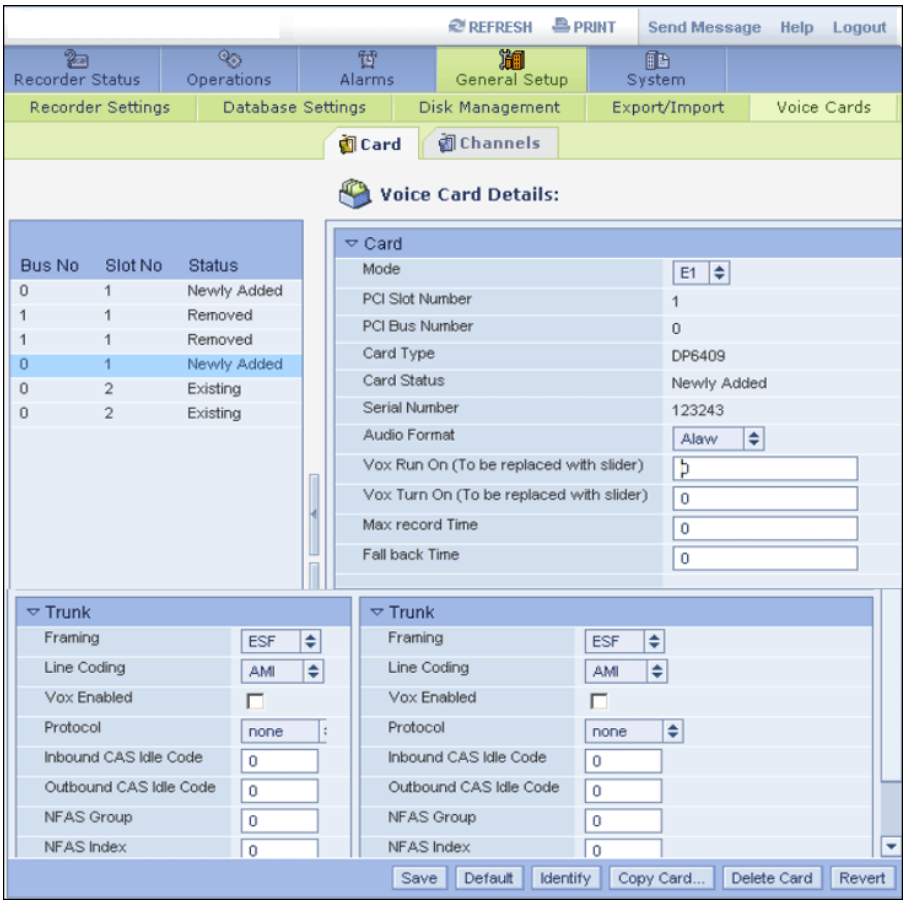
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Replacing a Voice Card

Replace a voice card as a replacement for a broken voice card in the same bus slot. The replacement card must be the same type, must be in the same slot, and must have a status of Replaced. You then update and save the setting. The fields on the voice cards vary according to card type selected.

To replace a voice card:

1. Complete the steps as described in Performing General Voice Card Tasks on page 111, and then click **General Setup > Voice Cards > Card**.
2. In the List box (left pane), select the replacement card. This card has a status of **Replaced**. You cannot edit the card until the card is saved and the status is **Existing**.



3. Click **Save**. The status of the card is changed from **Replaced** to **Existing**. You can now edit the card.
4. Complete the Voice Card Details screen fields for the card type by referring to one of the following:

- Modifying T1/E1 Voice Card Properties on page 122,

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- Modifying PCM32 Voice Card Properties on page 130,
- Modifying NGX Voice Card Properties on page 135,
- Modifying Cybertech Voice Card Properties on page 142,
- Modifying Analog Voice Card Properties on page 149.

Modifying the Properties of an Existing Voice Card

Modify an existing card to implement any card or channel configuration changes to either an E1/T1, NGX, or Analog voice card. In modifying an existing card, you select the card, make changes, save the changes, and the new settings take place upon restart of the Recorder service.

To modify an existing voice card:

1. Complete the steps as described in Adding a New Voice Card on page 115, and then click **General Setup > Voice Cards > Card**.
2. In the Voice Card List box (left pane), select the card (with the status of **Existing**) to be modified and type the new settings for the card type as by referring to one of the following:

- Modifying T1/E1 Voice Card Properties on page 122,
- Modifying PCM32 Voice Card Properties on page 130,
- Modifying NGX Voice Card Properties on page 135,
- Modifying Cybertech Voice Card Properties on page 142,
- Modifying Analog Voice Card Properties on page 149.

3. Click **Channels**, and review channel details if necessary, as described in Updating the Configuration of Voice Card Channels on page 118.
4. Click **Save** and reboot the system by clicking **Operations > Start and Stop** if prompted for the new settings take effect.

Viewing Voice Card Channels

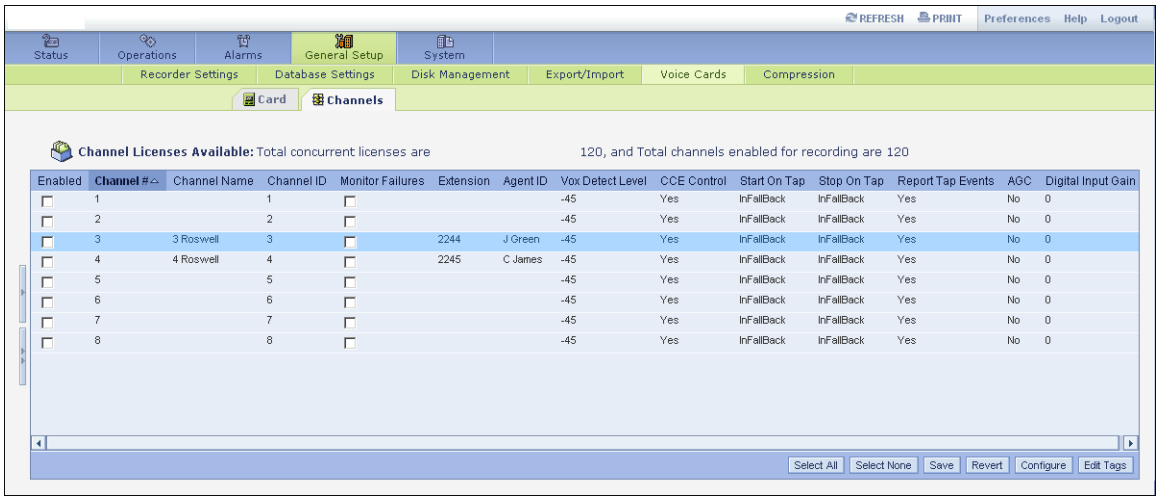
View voice card channels to review summary information of licensed channels corresponding to a selected voice card. Although channel configurations vary for each card type you can perform the same types of actions by clicking the action buttons to select, save, revert, configure, and identify cards.

To configure a channel, select any displayed channel and click **Configure**. Similarly, to copy a voice card configuration, select the card instead of the channel and then click **Copy Card.**

To view one or more voice card channels:

1. Choose **General Setup > Voice Cards** > **Card**.
2. In the Voice Card List box (left pane) select a voice card.
3. Click **Channels.** The Channel Licenses screen corresponding to the card displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



4 Configure channels by following procedures in Updating the Configuration of Voice Card Channels on page 118.

Updating the Configuration of Voice Card Channels

Update the configuration of a voice card channel to change properties such as channel numbers, IDs, and voice tap options. To update a voice card's channels, select the voice card in the Card tab, and click the Channels tab.

To update one or more voice card channels:

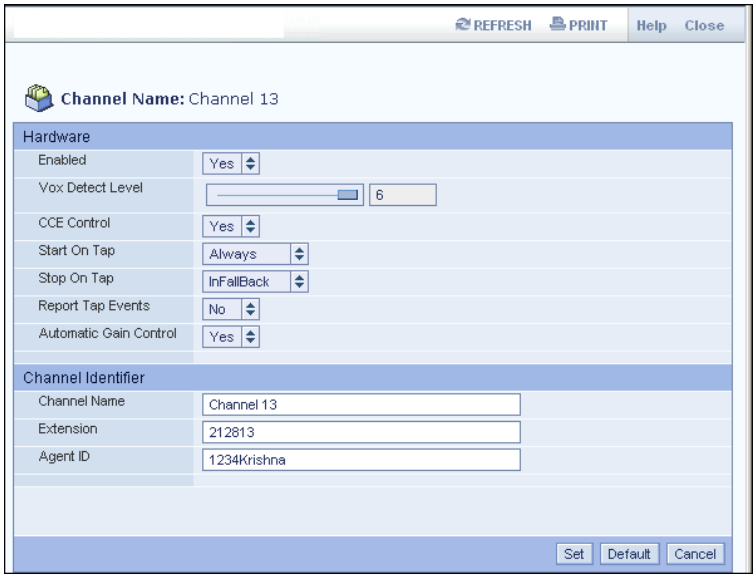
1 Review voice card channels by following procedures in Viewing Voice Card Channels on page 117**.** The Channel Licenses screen corresponding to the card type displays.

2 In the **Channel Licenses** screen, select one or more channels by doing one of the following:

- Click **Enabled** beside a channel to select and enable one or more channels
- Click **Select All** to select all channels,
- Click **Select None** to deselect a channel selection before selecting again.

3 Click **Configure**. The Channel details screen displays where settings will be applied for all selected channels.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



4 Complete the channel details screen according to the type of voice card selected:

- Updating T1/E1 Voice Card Channels on page 125.
- Updating PCM32 Voice Card Channels on page 132.
- Updating NGX Voice Card Channels on page 139.
- Updating Cybertech Voice Card Channels on page 146.
- Modifying Analog Voice Card Channels on page 150.

5 Click **Save** for each channel selected.

Editing Tags for Voice Card Channels

Edit voice card channel tags to assign a name to channels, as well as, for some voice cards, identification for the extensions and agents associated with channels. You can select one or many channels and apply settings without having to cycle through individual channels.

To update one or more voice card channels:

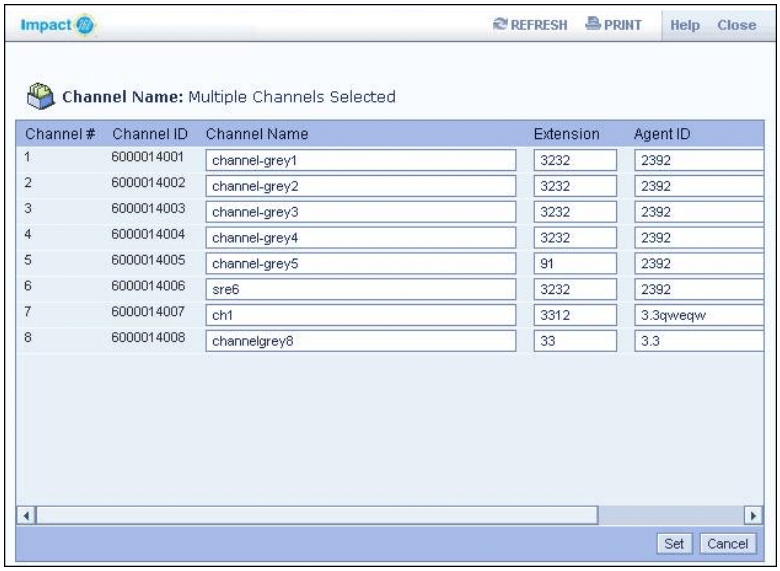
1 Review voice card channels by following procedures in Viewing Voice Card Channels on page 117**.** The Channel Licenses screen corresponding to the card type displays.

2 In the **Channel Licenses** screen, select one or more channels by doing one of the following:

- Click **Enabled** beside a channel to select and enable one or more channels.
- Click **Select All** to select all channels,
- Click **Select None** to deselect a channel selection before selecting again.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 Click **Edit Tags**. The channel details screen displays where you can type edit tag settings for all selected channels.


Impact
REFRESH
PRINT
Help
Close
Channel Name: Multiple Channels Selected
Channel # | Channel ID | Channel Name | Extension | Agent ID
1 | 6000014001 | channel-grey1 | 3232 | 2392
2 | 6000014002 | channel-grey2 | 3232 | 2392
3 | 6000014003 | channel-grey3 | 3232 | 2392
4 | 6000014004 | channel-grey4 | 3232 | 2392
5 | 6000014005 | channel-grey5 | 91 | 2392
6 | 6000014006 | sre6 | 3232 | 2392
7 | 6000014007 | ch1 | 3312 | 3.3qweqw
8 | 6000014008 | channelgrey8 | 33 | 3.3
Set
Cancel

4 Complete the channel details screen, based on your selection of channels, according to the following:

Item	Description
Channel#	Shows the numeric, automatically-assigned channel number. (Read-only field). For more information, refer to Modifying the Trunk Protocol on a T1 Voice Card on page 127.
Channel ID	Shows the numeric, automatically-assigned channel ID based on the serial number of the voice card. (Read-only field)
Channel Name	Type the name for the channel
Extension	Type the telephone extension associated with the channel.
Agent ID	Type the description (tag) of the agent associated with the telephone extension.

5 Click **Set**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring T1/E1 Voice Cards

Configuring the digital T1/E1 voice cards describes properties, trunks, and channels in T1/E1 voice cards and how to modify them. This information is described in the following topics:

- Modifying T1/E1 Voice Card Properties
- Updating T1/E1 Voice Card Channels
- Modifying the Trunk Protocol on a T1 Voice Card
- Modifying the Trunk Protocol on a E1 Voice Card

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Modifying T1/E1 Voice Card Properties

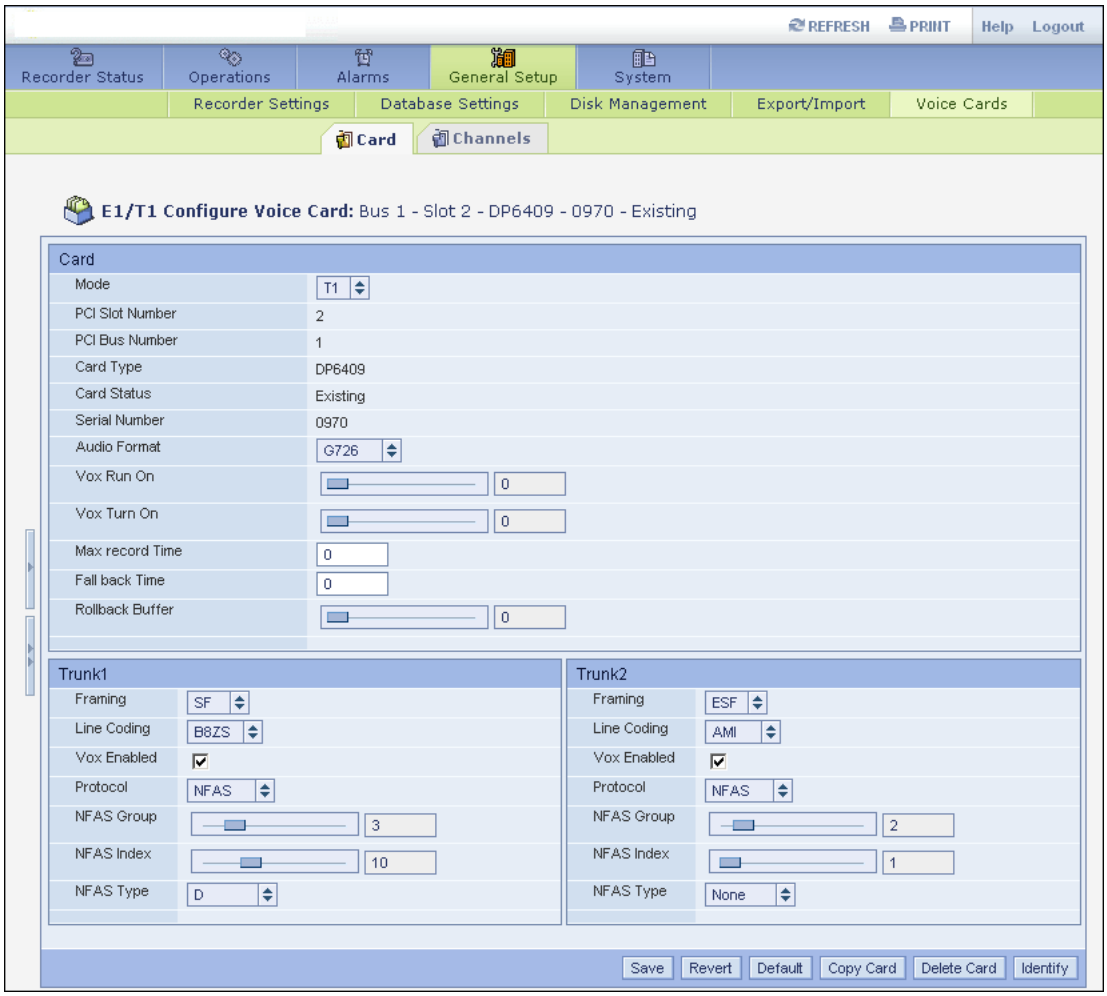
Modify an E1/T1 voice card with a status of Existing to implement any card property changes. To modify an E1/T1 card, you select the card in the Voice Card List pane on the left then make changes and save the changes in the right pane. The new settings take place upon reboot.

To modify a T1/E1 voice card:

1 Choose **General Setup > Voice Cards > Card**.

2 In the voice card list (left pane), select an T1/E1 voice cards with a status of **Existing**. Details display in the Card pane

Click the arrow buttons between screen panes to show and hide windows. For example, click the single arrow to view full screen only the list of voice cards. Click the double-arrows to view full screen the voice card properties together.



© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 Complete the E1/T1 properties in the card pane of the upper portion of the screen, according to the following:

Field	Description *
PCI Bus Number	The Bus Number on the PC's motherboard.
PCI Slot Number	The slot number on the PC's motherboard.
Data Source	Choose from the list the Data Source such as a Phone switch, to which this card is associated.
Member Group	Choose from the list the Data Source Member Group to which this card belongs
Card Type	The model number of the voice card. (DP3209, DP6409).
Serial #	The serial number of the voice card.
Card Status	Voice card status, namely (Newly Added, Replaced, Removed, Existing).
Mode	Defines whether the card is operating with the E1 or T1 firmware on it. Predefined options are E1 or T1 (T1 is the default). This field is editable and required.
Audio Recorded Format	Defines the method for encoding the audio data in a WAV file. Predefined options are Alaw, uLaw, G726, G729A (default), . This field is editable and required.
Input Companding Type	Defines the method for encoding the audio data in a WAV file. Predefined options are Alaw and uLaw.
VOX Run On (ms)	Defines the length of time in milliseconds that sound needs to be below the threshold before the VOX method determines a call has ended. Threshold is configurable on each channel. The number range is 0-13,000 (default 5,000). Increments are 91. For example, click the arrows once and the counter is increased/decreased by 91. This field is editable and required. See also Completing the VOX Tutorial on page 157
VOX Turn On (ms)	Defines the length of time in milliseconds that sound needs to be above the threshold before the VOX method identifies a call. Threshold is configurable on each channel. This is a numerical field that can be updated. The number can range from 0-4,000 (default is 250). Increments are 28. For example, click the arrows once and the counter is increased/decreased by 28. This field is editable and required
Max. Record Time (sec)	The maximum time in seconds that the call can be recorded. Default time is 3600 seconds. This field is optional.
Fall Back Time (sec)	Maximum elapsed time in seconds before the Recorder switches to **tap sense** mode if there is a loss of CTI feed. Default is zero seconds. This field is editable and required.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Rollback Buffer	Shows a value measured in milliseconds (0-1,000) that allows you to configure a number of milliseconds (default is 1,000) to automatically capture voice for a period before the start record command comes in. This allows the Recorder to compensate for delays in CTI or Unify processing and automatically rollback the voice and start recording for a brief amount of time before the actual start record request is received. This is a required field.
* All fields read only unless otherwise noted.	

4 Complete the T1/E1 trunk properties (Trunk pane in lower portion of screen) according to the following:

Field	Description *
Data Source	Choose the phone switch or LAN to which the voice card is connected.
Member Group	Shows the parent trunk span group, if any, for the Data Source
Framing	Describes the method used to "frame" the signal's stream of data bits into a series of multiplexed channels. Applicable always. Predefined options are "SF" or "ESF" for T1 mode (SF is the default for T1 mode) "G704" or "CRC" for E1 mode (G704 is the default for E1 mode).
Line Coding	Describes the method used to translate digital data into an electrical signal. Applicable always. Predefined options are "AMI" or "B8ZS" for T1 mode (AMI is the default), and "AMI" or "HDB3" for E1 mode (HDB3 is the default).
VOX Enabled	Describes whether the VOX method for call recording is enabled. Options are True and False. Default is False.
Protocol	Describes the multiplexing protocol used, such as ISDN or NFAS. This field is applicable always and will affect the availability of other fields. Predefined options are "Non-ISDN" (default), "ISDN", and "NFAS".
Data Source (does not appear on all screens)	Describes the association of Data Source with the Recorder. Options are all of the displayed associated Phone Data Sources. **Please Select** displays when the Recorder is not associated with any spans. This is an optional field. **Note**: This field displays only if the Recorder is associated to a Span in Enterprise Manager.
Span (does not appear on all screens)	Describes the association of Data Source trunk span with the E1/T1 trunk. This is based on selected Data Source (above). Options are all of the associated Data Source trunk spans with the Data Source which have not been assigned on the same card. *Please Select* displays when the Recorder is not associated with any spans. This is an optional field. **Note**: This field displays only if the Recorder is associated to a Span in Enterprise Manager.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Inbound CAS Idle Code	Defines the two-bit pattern used by the transmitting switch to indicate "on-hook" for the inbound signal. Applicable only when the protocol is "Non-ISDN" and the recording method is not VOX. Predefined options are 0-15 (0 is the default). (CAS is an abbreviation for Channel Associated Signalling).
Outbound CAS Idle Code	Defines the two-bit pattern used by the transmitting switch to indicate "on-hook" for the outbound signal. Applicable only when protocol is "Non-ISDN" and the recording method is not VOX. Predefined options are 0-1,111 (0 is the default). (CAS is an abbreviation for Channel Associated Signalling).
NFAS Group	Identifies the NFAS (Non-Facility Associated Signalling) group of which the span is a member. Applicable only when protocol is NFAS. Predefined options are 0-31 (0 is the default). Required for the applicable protocol setting.
NFAS Index	Identifies the span within an NFAS group. Applicable only when protocol is NFAS. Predefined options are 0-31 (0 is the default). Required for applicable protocol setting.
NFAS Type	Identifies whether the span is used for voice-only or whether it contains the D-Channel for the group or the backup D-channel for the group. Applicable only when protocol is NFAS. Predefined options are "D", "Backup" or "None" (None is the default). Required for applicable protocol setting.
* All fields required unless noted otherwise.	

5 Click **Channel** to configure the E1/T1 channels associated with this card, as described in Updating the Configuration of Voice Card Channels on page 118

6 Click **Save** when finished.

Updating T1/E1 Voice Card Channels

Update channels on the T1/E1 voice card to enable individual channels and modify recording settings for them. Channel IDs are created automatically. T1 cards can have a maximum of 24 channels (23 regular channels plus a d-channel) and E1 cards can have a maximum of 30 channels (29 regular channels plus a d-channel). The number of channels depends on the selection of T1 or E1 in the Card properties. For hands-on scenarios with channels, refer to Modifying the Trunk Protocol on a T1 Voice Card on page 127.

To modify T1/E1 voice card channels:

1 Choose **General Setup > Voice Cards** and select a T1/E1 card.

2 Click **Channels**. A list of all channels associated with the card type displays.

3 Review the displayed Channels according to the following:

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Enable Checkbox	Checkbox that determines whether a channel has been selected for use. Selecting the checkbox will subtract a license channel from the "Available License" counter and vice versa when a channel is unchecked. **Note**: The default value for checkboxes for cards with a status of **Newly Added** is unchecked (disabled).
Channel #	Number of the channel on the card, such as 1, 2, or 3. The DP3209 and DP6409 have 30 and 60 channels available respectively. This is a read-only field
Channel ID	Logical channel ID is a unique number that is used in the Unify mapping table to identify Channel. This is a unique number within the Recorder. This is a read-only field.
VOX Detect Level (DB)	Defines the threshold in decibels used for VOX-based call detection. The adjustable range is -48 to 6, with the default value of -45 (minus 45). Increments are 3. For example, clicking the thumbwheel arrows increases/decreases values by 3.
Monitor Failures	Checkbox option to specify whether this channel is monitored for failure. If this option is selected, a channel failure indication alarm is sent when this channel fails to record calls. If unchecked, the channel failure does not show as an alarm.
CCE Control	Shows options for the Command Control Engine (Unify). Options are **True** and **False. True** is the default.
Start On Tap	Indicates that recording begins when tapping of the channel begins. Options are **Always**, **Never**, and **In Fall Back**. Default is **In Fall Back**. See also Completing the VOX Tutorial on page 157
Stop on Tap	Indicates that recording stops when tapping of the channel begins. Options are **Always**, **Never**, and **In Fall Back**. Default is **In Fall Back**.
Report Tap Events	Indicates whether start and stop events triggered from VOX or D-channel detection on the telephony card are passed to the Command Control Engine (Unify or Integration Framework). Options are **True** and **False**, default **True**. For systems where VOX or D-channel (including fallback) is not being used, this setting can be set to **False** to reduce the number of events that have to be processed by the Command Control Engine, thereby reducing the processing load on the system.
Auto Gain Control (AGC)	Enables an option on the voice card to automatically amplify the voice on the channel when necessary. Options are **True** or **False**. Default is **False**.
Digital Input Gain	Defines a level of amplification that can be used on weak channels. Number range is from -3 (minus 3) to 24. 0 is the default. Increments are in one. For example, clicking the thumbwheel arrows increases/decreases the value by one.
* All fields are required except where otherwise noted.	

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

4 Select a channel, click **Configure**, and complete the Configure Voice Card window as described in Updating the Configuration of Voice Card Channels on page 118.

5 Click **Save**. The changes you made to the channel are saved in the Recorder's **`configuration.xml`** file.

6 Click **Operation > Start and Stop**, select Recorder, and click **Restart** to restart the Recorder.

Modifying the Trunk Protocol on a T1 Voice Card

Modify the trunk protocol in a T1 voice card to determine the signalling variant, and therefore the number of channels available, to be used as a line protocol. See also Modifying T1/E1 Voice Card Properties on page 122 for more information on trunks and protocols.

To modify the protocol on a T1 card:

1 With a T1 voice card selected, choose **General Setup > Voice Cards > Card** and in the Trunk pane choose a Protocol according to the following:

Protocol	Description	Channels Available
ISDN	Integrated Services Digital Network (ISDN) is a signaling variant used with the T1 or E1 that reserves a single data channel on each multiplexed line for signaling information.	23
Non-ISDN	Applies to CAS (Channel Associated Signaling) or RBS (Robbed Bit Signaling) which are signalling variants used with the T1 or E1 that reserves a single data channel on each multiplexed line for signaling information.	24
NFAS D	This is a variant of ISDN used with T1 where a single D-channel is used to service up to 10 x T1 lines.	23
NFAS Backup	This is a variant of ISDN used with T1 where a backup channel, not necessarily the D-channel, is used to service up to 10 x T1 lines.	23
NFAS None	A non-facility associated signaling variant of ISDN used with T1 lines but which does not use a D-channel or Backup channel.	24
Note: Channels available are doubled if a DP6409 card is used as two trunks are available with this card.		

2 Click **Channels** to view the number of channels available after the update.

If you have exceeded the number of licensed channels, you must obtain additional licenses.

3 Click **Save**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

4 Click **Operations > Start and Stop > Reboot** when prompted to restart the Recorder PC. Changes take effect after the restart.

Modifying the Trunk Protocol on a E1 Voice Card

Modify the trunk protocol in an E1 Card to determine the signalling variant, and therefore the number of channels available, to be used as a line protocol. See also Modifying T1/E1 Voice Card Properties on page 122 for more information on properties and channels.

To modify the protocol in a E1 voice card:

1 With an E1 voice card selected, choose **General Setup > Voice Cards > Card** and in the Trunk pane choose a Protocol according to the following:

Protocol	Description	Channels Available
ISDN/ DASS2	Integrated Services Digital Network (ISDN) is a signalling variant used with the T1 or E1 that reserves a single data channel on each multiplexed line for signaling information. DASS2 is a predecessor of ISDN.	30/60
None	Applies to CAS (Channel Associated Signaling) and RBS (Robbed Bit Signaling) which are signalling variants used with the T1 or E1 that reserves a single data channel on each multiplexed line for signaling information.	30/60
DPNSS	The Digital Private Network Signalling System (DPNSS) is a network protocol used on digital trunk lines for connecting two PBXs. DPNSS supports a defined set of inter-networking facilities.	30/60
Note: Channels available are for the DP3209 and DP6409 respectively (channels are doubled if a DP6409 card is used as two trunks are available with this card).		

2 Click **Channels** to view the number of channels available after the update. If you have exceeded the number of licensed channels, you must obtain additional licenses.

3 Click **Save**.

4 Click **Operations > Start and Stop > Reboot** when prompted to restart the Recorder PC. Changes take effect after the restart

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring PCM32 Voice Cards

Configuring PCM32 voice cards describes properties and channels in the digital PCM32 voice cards and how to modify them. Like the T1/E1 card, the PCM32 is trunk-based and is used in trading environments such as stocks, bonds and commodity trading. The PCM32 protocol is similar to E1 in that it is cabled over twisted pair cable and terminated with RJ-45 connectors. The card supports 32 voice channel per trunk span. Two models, both from Ai-Logix, are supported: the PCM3209, which is a single trunk span card, and the PCM6409, which is a dual trunk-span card. Information is described in the following topics:

- Modifying PCM32 Voice Card Properties
- Updating PCM32 Voice Card Channels
- Viewing PCM32 Channel Identifiers

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

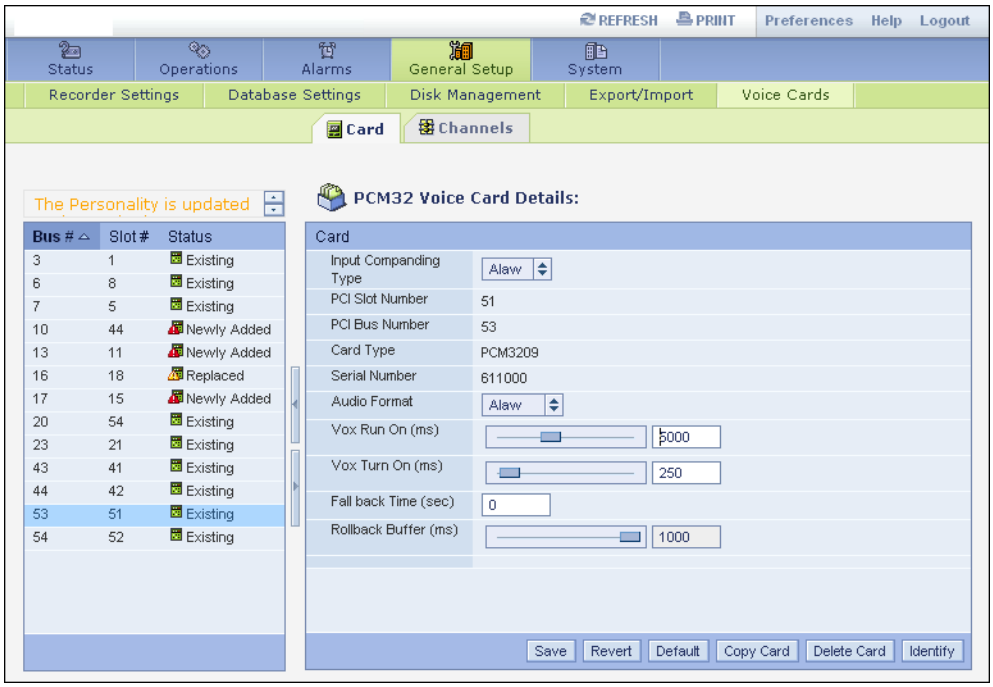
Modifying PCM32 Voice Card Properties

Modify a PCM32 voice card with a status of Existing to implement any card property changes. To modify a PCM32 card, you select the card in the Voice Card List pane on the left then make changes and save the changes in the right pane. Most configuration changes take effect dynamically without restarting the capture engine or rebooting the Recorder, except for changes to the Input Companding Type. Changes to this require a rebooting of the system.

To modify a PCM32 voice card:

1 Choose **General Setup > Voice Cards > Card**.

2 In the voice card list (left pane), select a PCM32 voice cards with a status of **Existing**. Details display in the Card pane.



3 Complete the PCM32 properties according to the following:

Field	Description *
Input Companding Type	Defines the method for encoding the audio data in a WAV file. Predefined options are Alaw and uLaw.
PCI Bus Number	The Bus Number on the PC's motherboard.
PCI Slot Number	The slot number on the PC's motherboard.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Data Source	Choose from the list the Data Source such as a Phone switch, to which this card is associated.
Member Group	Choose from the list the Data Source Member Group to which this card belongs
Card Type	The model number of the voice card. (DP3209, DP6409).
Serial #	The serial number of the voice card.
Card Status	Voice card status, namely (Newly Added, Replaced, Removed, Existing).
Audio Recorded Format	Defines the method for encoding the audio data in a WAV file. Predefined options are Alaw, uLaw, G726 (default), G729A (the default). This field is editable and required.
VOX Run On (ms)	Defines the length of time in milliseconds that sound needs to be below the threshold before the VOX method determines a call has ended. Threshold is configurable on each channel. The number range is 0-13,000 (default 5,000). Increments are 91. For example, click the arrows once and the counter is increased/decreased by 91. This field is editable and required. See also Completing the VOX Tutorial on page 157
VOX Turn On (ms)	Defines the length of time in milliseconds that sound needs to be above the threshold before the VOX method identifies a call. Threshold is configurable on each channel. This is a numerical field that can be updated. The number can range from 0-4,000 (default is 250). Increments are 28. For example, click the arrows once and the counter is increased/decreased by 28. This field is editable and required
Fall Back Time (sec)	Maximum elapsed time in seconds before the Recorder switches to **tap sense** mode if there is a loss of CTI feed. Default is zero seconds. This field is editable and required.
Rollback Buffer	Shows a value, measured in milliseconds (0-1,000), that allows the user to configure a number of milliseconds (default is 1,000) to automatically capture voice for a period before the start record command comes in. This allows the Recorder to compensate for delays in CTI or Unify processing and automatically rollback the voice and start recording a brief amount of time before the actual start record request is received. This is a required field.
Data Source	Choose the phone switch or LAN to which the voice card is connected.
Member Group	Shows the parent trunk span group, if any, for the Data Source

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Termination Impedance	Determines whether the span will be terminated with Low Impedance for normal connections or High Impedance for N+N redundant Recorder configurations. Values are **Low (Single Recorder)** and **High (N+N Redundant Recorders)**. **Note:** N+N refers to having one backup Recorder for each Recorder in a system. So if you would normally need 5 Recorders to cover a particular number of channels, you would deploy 10 instead: 5 primary and 5 backup Recorders.
* All fields read only unless otherwise noted.	

4 Click **Channel** to configure the E1/T1 channels associated with this card, as described in Updating the Configuration of Voice Card Channels on page 118

5 Click **Save** when finished.

Updating PCM32 Voice Card Channels

Update channels on the PCM32 voice card to enable individual channels and modify recording settings for them. Channel IDs are created automatically. PCM32 cards can have a maximum of 32 channels (PCM3209 card) and 64 channels (PCM6409). For hands-on scenarios with channels, refer to Modifying the Trunk Protocol on a T1 Voice Card on page 127.

To modify PCM32 voice card channels:

1 Choose **General Setup > Voice Cards** and select a PCM32 card.

2 Click **Channels**. A list of all channels associated with the card type displays.

3 Review the displayed Channels according to the following:

Field	Description *
Enable Checkbox	Checkbox that determines whether a channel has been selected for use. Selecting the checkbox will subtract a license channel from the "Available License" counter and vice versa when a channel is unchecked. **Note**: The default value for checkboxes for cards with a status of **Newly Added** is unchecked (disabled).
Channel #	Number of the channel on the card, such as 1, 2, or 3. The DP3209 and DP6409 have 30 and 60 channels available respectively. This is a read-only field
Channel ID	Logical channel ID is a unique number that is used in the Unify mapping table to identify Channel. This is a unique number within the Recorder. This is a read-only field.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
VOX Detect Level (DB)	Defines the threshold in decibels used for VOX-based call detection. The adjustable range is -48 to 6, with the default value of -45 (minus 45). Increments are 3. For example, clicking the thumbwheel arrows increases/decreases values by 3.
Max Record Time (sec)	This defines the maximum time in seconds that a channel will spend in the Recording state before forcing a break. Maximum is 1200. This is used in trading environments to limit the size of WAV files on continuously recording channels. This setting has been moved from the card level to the individual channel level to allow more flexibility in trading environments. This field is optional.
Monitor Failures	Checkbox option to specify whether this channel is monitored for failure. If this option is selected, a channel failure indication alarm is sent when this channel fails to record calls. If unchecked, the channel failure does not show as an alarm.
CCE Control	Shows options for the Command Control Engine (Unify). Options are **True** and **False. True** is the default.
Start On Tap	Indicates that recording begins when tapping of the channel begins. Options are **Always**, **Never**, and **In Fall Back**. Default is **In Fall Back**. See also Completing the VOX Tutorial on page 157
Stop on Tap	Indicates that recording stops when tapping of the channel begins. Options are **Always**, **Never**, and **In Fall Back**. Default is **In Fall Back**.
Report Tap Events	Indicates whether start and stop events triggered from VOX or D-channel detection on the telephony card are passed to the Command Control Engine (Unify or Integration Framework). Options are **True** and **False**, default **True**. For systems where VOX or D-channel (including fallback) is not being used, this setting can be set to **False** to reduce the number of events that have to be processed by the Command Control Engine, thereby reducing the processing load on the system.
Auto Gain Control (AGC)	Enables an option on the voice card to automatically amplify the voice on the channel when necessary. Options are **True** or **False**. Default is **False**.
Digital Input Gain	Defines a level of amplification that can be used on weak channels. Number range is from -3 (minus 3) to 24. 0 is the default. Increments are in one. For example, clicking the thumbwheel arrows increases/decreases the value by one.
* All fields are required except where otherwise noted.	

4 Select a channel, click **Configure**, and complete the Configure Voice Card window as described in Updating the Configuration of Voice Card Channels on page 118.

5 Click **Save**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Viewing PCM32 Channel Identifiers

The following information displays when you configure an individual channel. These fields, also known as static tags, are configurable only on the individual card level. That is, identifiers apply to the selected card only.

Field	Description
Channel Name	User definable channel name (alphanumeric). Optional field

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring NGX Voice Cards

Configuring NGX voice cards describes properties and channels in the Ai-Logix NGX model of voice cards and how to modify them. The NGX card records digital, station-side calls, and uses a combination of connector hardware and punchdown blocks. Compatible models appear in Compatible Voice Cards. Information is described in the following topics:

- Modifying NGX Voice Card Properties
- Updating NGX Voice Card Channels
- Viewing NGX Channel Identifiers

Modifying NGX Voice Card Properties

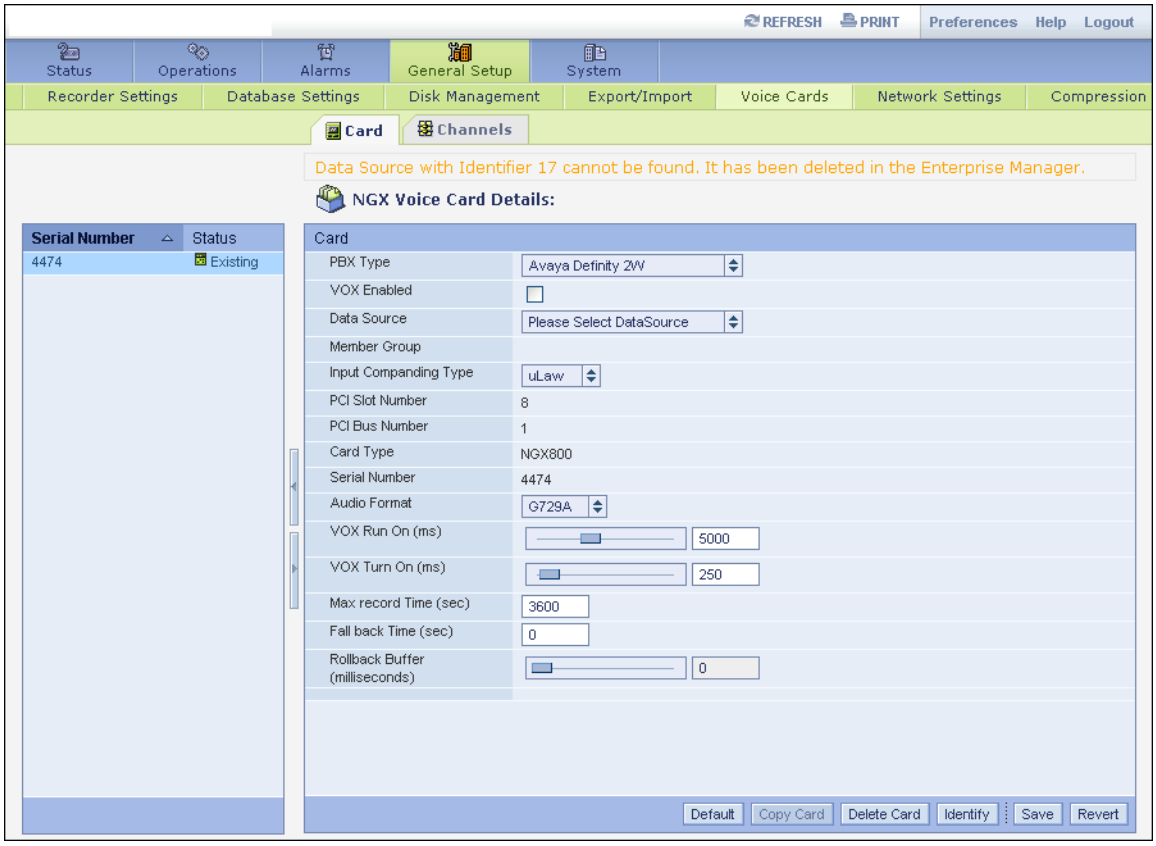
Modify an NGX voice card with a status of Existing to implement any voice card property changes. NGX cards record digitally on the station-side (extension) of the trunk, unlike T1/E1 cards, which record digitally on the trunk (switch) side. To modify an NGX card, you select the card in the voice card list in the left pane then make changes and save the changes in the right pane. The new settings take place upon restart of the Recorder, if prompted.

To modify a NGX voice card:

1 Choose **General Setup > Voice Cards > Card**.

2 In the voice card list (left pane), select an NGX voice card with a status of **Existing**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



3 Review NGX voice card properties and make changes according to the following:

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
PBX Type	Choose from list the type of PBX switch that the Recorder is interfacing with. Options include: **Alcatel 4200/4400** **Aspect** **Avaya Definity 2W** **Avaya Index** **Avaya MLX** **Avaya Definity 4W** **Avaya Merlin Magix** **Bosch Integral 2W** **Bosch Integral 4W** **Bosch Integral 55** **BRI ISDN** **Ericsson ELU25** **Ericsson ELU5** **Fujitsu F9600** **Intecom EADS 2W** **Intecom EADS 4W** **Inter-Tel** **LG Starex CS** **NEC** **Nortel Matra** **Nortel Meridian1** **Nortel Norstar** **Philips SOPHO iS3000 2W** **Philips SOPHO iS3000 4W** **Rockwell Spectrum** **Samsung DCS828** **Siemens Hicom** **Siemens RolmLINK** **Toshiba Strata DK** **eOn eQueue** **Mitel Sx2000** **Panasonic TDA-50** **Ascotel Intelligate** **BRI ISDN NI1** **Panasonic 7600 Special** **Samsung INFOREX** **Siemens Realitis DTI 4W** **Siemens Realitis iSDT 2W** **Tadiran Coral** **Teltronics (Harris2020)**
VOX enabled	Describes whether the VOX method for call recording is enabled. Options are **True** and **False**. Default is **False**. Required updateable field

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Data Source	Choose the phone switch or LAN to which the voice card is connected.
Member Group	Shows the station-side group, if any, for the Data Source.
Input Companding Type	Choose the method for encoding the audio data in a WAV file. Options are Alaw and uLaw.
PCI Bus Number	The Bus Number on the PC's motherboard.
PCI Slot Number	The Slot Number on the PC's motherboard.
Card Type	NGX Voice Card Model Number (NGX800, NGX1600, NGX2400). You can add an NGX80 daughterboard that increases the channel capacity of the card. **Note:** in Windows device manager the card shows as NGX800.
Serial Number	The unique serial number of the voice card.
Card Status	The status of the voice card, namely **Newly Added, Replaced, Removed,** or **Existing**.
Audio Format	Defines the method for encoding the audio data in a WAV file. Predefined options are Alaw, uLaw, G726 , G729A (the default). This field is editable and required.
VOX Run On (ms)	Defines the length of time in milliseconds that sound needs to be below the threshold before the VOX method determines a call has ended. Threshold is configurable on each channel. Number range is 0-13,000 (default is 5,000). Increment value is 91. For example, clicking the thumbwheel arrows increases/decreases displayed values by 91. This field is editable and required. See also Completing the VOX Tutorial on page 157
VOX Turn On (ms)	Defines the length of time, in milliseconds, that sound needs to be above the threshold before the VOX method identifies a call. Threshold is configurable on each channel. Number range is 0-4,000 (default is 250). Increment value is 28. For example, clicking the thumbwheel arrows increases/decreases displayed values by 28. This field is editable and required.
Max Record Time (sec)	Maximum record time in seconds for a single call segment. Default is 3600 seconds. This field is editable and required
Fall Back Time (sec)	Maximum elapsed time in seconds before the Recorder switches to **tap sense** mode if there is a loss of CTI feed. Default is zero seconds. This field is editable and required
Rollback Buffer (ms)	Shows a value that is a measure in milliseconds (0-1,000). Allows the user to configure a number of milliseconds (default is 1,000) to automatically capture voice for a period before the start record command comes in. This allows the Recorder to compensate for delays in CTI or Unify processing and automatically rollback the voice and start recording a brief amount of time before the actual start record request is received. This is a required field.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Data Source (does not appear on all screens)	Describes the association of Data Source with the Recorder. Options are all of the displayed associated Data Sources. **Please Select** displays when the Recorder is not associated with any spans. This is an optional field. **Note**: This field displays only if the Recorder is associated to a Span in Enterprise Manager.
Span (does not appear on all screens)	Describes the association of Data Source trunk span with the E1/T1 trunk. This is based on selected Data Source (above). Options are all of the associated Data Source trunk spans with the Data Source which have not been assigned on the same card. **Please Select** displays when the Recorder is not associated with any spans. This is an optional field. **Note**: This field displays only if the Recorder is associated to a Span in Enterprise Manager.
* Fields are read only unless otherwise stated.	

4 Click **Save** when finished.

5 Click **Operations > Start and Stop,** select **Recorder** and click **Restart** when requested to restart the Recorder.

Updating NGX Voice Card Channels

Update channels on the NGX voice card to enable individual channels and modify recording settings for them. Channel IDs are created automatically. The number of channels available depends on the type of card, as described in Compatible Voice Cards on page 242. For hands-on scenarios with channels, refer to Modifying the Trunk Protocol on a T1 Voice Card on page 127.

To modify NGX voice card channels:

1 Choose **General Setup > Voice Cards** and select a NGX card.

2 Click **Channels**. A list of all channels associated with the card type displays.

3 Review the displayed Channels according to the following:

Field	Description *
Enable Checkbox	Field that determines whether a channel has been selected for use. Selecting the checkbox subtracts a license channel from the "Available License" counter and vice versa when a channel is unchecked. **Note**: For cards with a status of **Newly Added** all channels are unchecked (i.e. disabled).
Channel Number	Number of the channel on the card such as 1, 2, 3 etc. Read-only field.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Channel ID	Logical channel ID that will be used in the Unify mapping table to identify a Channel. This is a unique number within the Recorder. That is, all channels in a Recorder have a unique number that is generated from the card auto-detect process. Read-only field.
VOX Detect Level	Defines the threshold used for VOX-based call detection. Units are in decibels. This is a numeric field that is updateable. Number range is from -57 (minus 57) to 6. -45 is the default. Increments are in values of 3. For example, clicking the thumbwheel arrows increases/decreases values by a factor of 3.
Monitor Failures	Checkbox option to specify whether this channel is monitored for failure. If this option is selected, a channel failure indication alarm is sent when this channel fails to record calls. If unchecked, the channel failure does not show as an alarm.
CCE Control	Shows options for the Command Control Engine (Unify). Options are **True** and **False. True** is the default.
Start On Tap	Indicates that recording begins when tapping of the channel begins. Options are **Always**, **Never**, and **In Fall Back**. Default is **In Fall Back**.
Stop on Tap	Indicates that recording stops when tapping of the channel begins. Options are **Always**, **Never**, and **In Fall Back**. Default is **In Fall Back**.
Report Tap Events	Indicates whether start and stop events triggered from VOX or D-channel detection on the telephony card are passed to the Command Control Engine (Unify or Integration Framework). Options are **True** and **False**, default **True**. For systems where VOX or D-channel (including fallback) is not being used, this setting can be set to **False** to reduce the number of events that have to be processed by the Command Control Engine, thereby reducing the processing load on the system.
Auto Gain Control	Enables an option on the voice card to automatically amplify the voice on the channel when necessary. Options are **True** or **False**. Default is **False**.
Start Record Events	Default is "event off hook". This field is not displayed on the Recorder Manager and the configuration is hard coded on a per client basis during the install. Additional values are customized depending on client needs.
Stop Record Events	Default is "event off hook". Same as Start Record Events above.
Digital Input Gain	Defines a level of amplification that can be used on weak channels. This is a numerical field that is updateable. Number range is from -3 (minus 3) to 24. Zero is the default. Increments are in values of 1. For example, click the thumbwheel arrows and the display increases/decreases by a factor of 1.
* All fields are required unless otherwise indicated.	

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

4 Select a channel, click **Configure**, and complete the Configure Voice Card window as described in Updating the Configuration of Voice Card Channels on page 118.

5 Click **Save**.

6 Click **Operation > Start and Stop**, select **Recorder**, and click **Restart** to restart the Recorder if prompted.

Viewing NGX Channel Identifiers

The following information displays in the lower pane (Trunk pane) of the configure window when you configure an individual channel. These fields, also known as static tags, are configurable only on the individual card level. That is, identifiers apply to the selected card only.

Field	Description
Channel Name	User definable channel name (alphanumeric). Optional field
Extension	Extension number (numeric). Optional field
Agent ID	Agent Identifier. (Alphanumeric). Optional field.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Cybertech Voice Cards

Configure Cybertech voice card properties and channels to set up and modify Cybertech digital extension tap (DET) voice cards. The Cybertech card records digital, station-side calls, and uses a combination of connector hardware and punchdown blocks. Compatible models appear in Compatible Voice Cards. Information is described in the following topics:

- Modifying Cybertech Voice Card Properties
- Updating Cybertech Voice Card Channels
- Using the Cybertech Update Personality Feature
- Viewing Cybertech Channel Identifiers

Modifying Cybertech Voice Card Properties

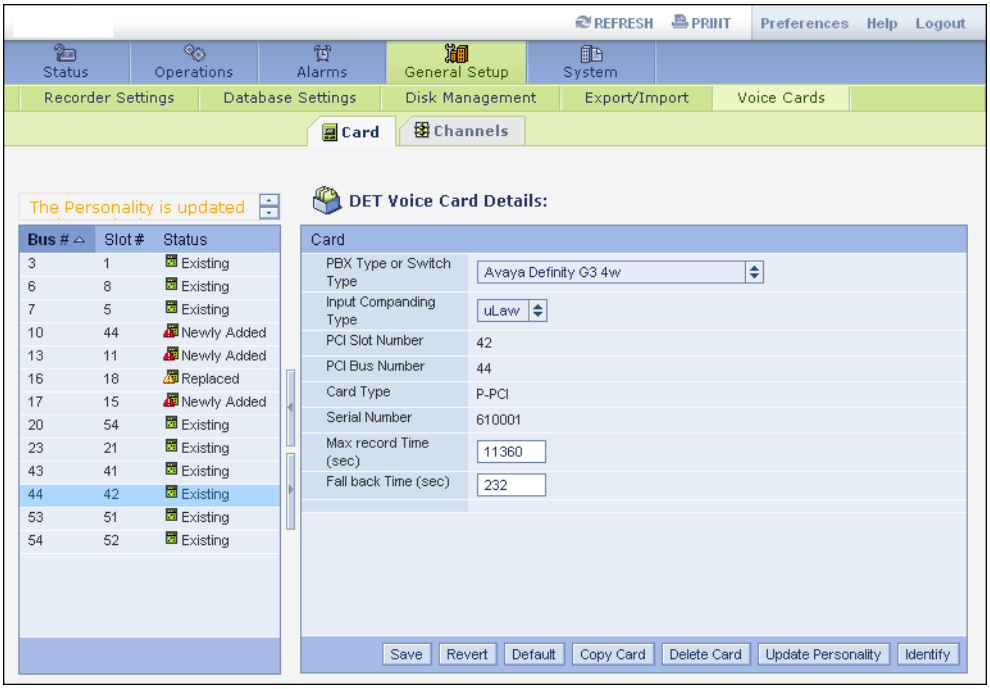
Modify a Cybertech voice card with a status of Existing to implement any voice card property changes. These cards record digitally on the station-side (extension) of the trunk, unlike T1/E1 cards, which record digitally on the trunk (switch) side. To modify a Cybertech card, select the card in the voice card list then make and save the changes in the right pane.

In some Cybertech cards, an **Update Personality** feature is available. See Using the Cybertech Update Personality Feature on page 148. This feature updates the personality file on the card's driver to allow communication with different switch types. **It is recommended that this feature not be used unless your are changing the switch type.**

To modify a Cybertech voice card:

1. Choose **General Setup > Voice Cards > Card**.
2. In the voice card list (left pane), select a Cybertech voice card with a status of **Existing**. The DET Voice Card Details window displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



3 Review Cybertech voice card properties and make changes according to the following:

Field	Description *
PCI Bus Number	The Bus Number on the PC's motherboard.
PCI Slot Number	The Slot Number on the PC's motherboard.
Card Type	Cybertech Voice Card Model Number (DSC16-PCI or DSC-MOD-PCI). You can add a digital or analog detection module (i.e. a daughterboard) that increases the channel capacity of the card. Each voice card supports a different set of switch types as shown under PBX/Switch types below.
Serial Number	The unique serial number of the voice card.
Card Status	The status of the voice card, namely **Newly Added, Replaced, Removed,** or **Existing**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
PBX Type or Switch Type (for DSC16-PCI).	The type of PBX switch that the Recorder is interfacing with. Options for the DSC16-PCI or DSC-MOD-PCI cards are given below. The following PBX/Switch types are supported by the DSC16-PCI: **Alcatel 4200/4400** **Ascom Ascotel** **Aspect CallCentre** **Avaya 5ESS** **Avaya Definity G3 2w** **Avaya Definity G3 42w** **Avaya Merlin Legend MLX series 2w** **Avaya Merlin Legend MLX series 4w** **Bosch Integral 2w** **Bosch Integral 4w** **Ericsson Business phone ELU25/28** **Ericsson MD110 ELU25/28** **Generic S0 (BRI)** **Generic U0P** **ISDN2 ETSI/ITR6** **NEC** **Nortel Matra** **Nortel Meridian M1 (default)** **Nortel Norstar** **Philips sopho 2w** **Philips sopho 4w** **Siemens Hicom** **Siemens Hipath** **Tadicom coral**

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
PBX Type or Switch Type for DSC-MOD-PCI.	The following PBX/Switch types are supported by the DSC-MOD-PCI: **Alcatel 4200/4400/OmniPCX** **Ascom Ascotel** **Aspect CallCentre** **Avaya 5ESS** **Avaya Definity G3 2w** **Avaya Definity G3 4w** **Avaya Merlin Legend MLX 2w** **Avaya Merlin Legend MLX 4w** **Avaya/Tenovis Integral 2w** **Avaya/Tenovis Integral 4w** **Bosch Integral 2w** **Bosch Integral 4w** **DMS-100 (bri)** **Ericsson Business phone ELU25/28** **Ericsson MD110 ELU25/28** **Fujitsu coral** **Generic S0 (bri)** **Generic Up0** **Intertel Axxess** **ISDN2 ETSI/ITR6** **LG Aria** **NEC** **NEC Aspire** **Nitsuko DX2E** **Nortel MatraNortel** **Meridian M1 (default)** **Nortel Norstar** **Panasonic KX-TD** **Philips Sopho 2w** **Philips Sopho 4w** **Realitis DX 4w** **Rockwell Spectrum 4w** **Siemens Hicom** **Siemens Hipath** **Siemens Hipath DX 4w** **Tadicom coral** **Toshiba Strata**
Input Companding Type	Defines the method for encoding the audio data in a WAV file. Predefined options are Alaw and uLaw. This field is editable and required.
Max Record Time (sec)	Maximum record time in seconds for a single call segment. Default is 3600 seconds. This field is editable and required

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Fall Back Time (sec)	Maximum elapsed time in seconds before the Recorder switches to **tap sense** mode if there is a loss of CTI feed. Default is zero seconds. This field is editable and required.
Data Source (does not appear on all screens)	Describes the association of Data Source with the Recorder. Options are all of the displayed associated Data Sources. **Please Select** displays when the Recorder is not associated with any spans. This is an optional field. **Note**: This field displays only if the Recorder is associated to a Span in Enterprise Manager.
Member Group (does not appear on all screens)	Describes the association of Data Source trunk span with the E1/T1 trunk. This is based on selected Data Source (above). Options are all of the associated Data Source trunk spans with the Data Source which have not been assigned on the same card. **Please Select** displays when the Recorder is not associated with any spans. This is an optional field. **Note**: This field displays only if the Recorder is associated to a Member Group in Enterprise Manager.
* Fields are read only unless otherwise stated.	

4 Click **Save** when finished.

5 Click **Channels** and configure channels as described in Updating Cybertech Voice Card Channels on page 146.

6 Click **Operations > Start and Stop,** select **Recorder** and click **Restart** when requested to restart the Recorder.

Updating Cybertech Voice Card Channels

Update channels on the Cybertech voice card to enable individual channels and modify recording settings for them. Channel IDs are created automatically. The number of channels available depends on the type of card, as described in Compatible Voice Cards on page 242. For hands-on scenarios with channels, refer to Modifying the Trunk Protocol on a T1 Voice Card on page 127.

To modify Cybertech voice card channels:

1 Choose **General Setup > Voice Cards** and select a Cybertech card.

2 Click **Channels**. A list of all channels associated with the card type displays.

3 Review the displayed Channels according to the following:

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description *
Enable Checkbox	Field that determines whether a channel has been selected for use. Selecting the checkbox subtracts a license channel from the "Available License" counter and vice versa when a channel is unchecked. **Note**: For cards with a status of **Newly Added** all channels are unchecked (i.e. disabled).
Channel Number	Number of the channel on the card such as 1, 2, 3 etc. Read-only field.
Channel ID	Logical channel ID that will be used in the Unify mapping table to identify a Channel. This is a unique number within the Recorder. That is, all channels in a Recorder have a unique number that is generated from the card auto-detect process. Read-only field.
Monitor Failures	Checkbox option to specify whether this channel is monitored for failure. If this option is selected, a channel failure indication alarm is sent when this channel fails to record calls. If unchecked, the channel failure does not show as an alarm.
CCE Control	Shows options for the Command Control Engine (Unify). Options are **True** and **False. True** is the default.
Start On Tap	Indicates that recording begins when tapping of the channel begins. Options are **Always**, **Never**, and **In Fall Back**. Default is **In Fall Back**. See also Completing the VOX Tutorial on page 157.
Stop on Tap	Indicates that recording stops when tapping of the channel begins. Options are **Always**, **Never**, and **In Fall Back**. Default is **In Fall Back**.
Report Tap Events	Indicates whether start and stop events triggered from VOX or D-channel detection on the telephony card are passed to the Command Control Engine (Unify or Integration Framework). Options are **True** and **False**, default **True**. For systems where VOX or D-channel (including fallback) is not being used, this setting can be set to **False** to reduce the number of events that have to be processed by the Command Control Engine, thereby reducing the processing load on the system.
PBX Vol.	Indicates the default volume of the PBX. Number range is -3 (minus 3) to 4. Zero is the default. Increments are 1. For example, clicking the thumbwheel arrows increases/decreases the displayed value by a factor of one.
Handset Vol.	Indicates the default volume on the handset. Number range is -3 (minus 3) to 4. Zero is the default. Increments are 1. For example, clicking the thumbwheel arrows increases/decreases the displayed value by a factor of one.
* All fields are required unless otherwise indicated.	

4 Select a channel, click **Configure**, and complete the Configure Voice Card window as described in Updating the Configuration of Voice Card Channels on page 118.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

5 Click **Save**. The changes you made to the channel are saved in the Recorder's **`configuration.xml`** file.

6 Click **Operation > Start and Stop**, select **Recorder**, and click **Restart** to restart the Recorder if prompted.

Using the Cybertech Update Personality Feature

Use the Update Personality feature in Cybertech cards only to update the personality file on the card's driver to allow communication with different switches. **It is strongly recommended that this option be used only when a switch type is changed.**

To use the update personality feature:

1 Choose **General Setup > Voice Cards > Card**.

2 In the voice card list (left pane), select a Cybertech voice card with a status of **Existing**. The DET Voice Card Details window displays.

3 Click **Update Personality**.

This operation may take several minutes to complete. Do not interrupt the download process.

4 Click **Operations > Start and Stop,** and then click **Reboot** to reboot when requested.

Viewing Cybertech Channel Identifiers

The following information displays in the lower pane (Trunk pane) of the configure window when you configure an individual channel. These fields, also known as static tags, are configurable only on the individual card level. That is, identifiers apply to the selected card only.

Field	Description
Channel Name	User definable alphanumeric channel name. Optional field
Extension	Extension number. Optional field
Agent ID	Agent Identifier. Optional field.

Configuring Analog Voice Cards

Configure any compatible analog voice card to add TDM recording parameters to that card or to change its channels' information. Two types of analog voice card are described: Ai-Logix and Cybertech. For compatible voice cards, refer to Compatible Voice Cards on page 242. This information is described in the following topics:

- Modifying Analog Voice Card Properties
- Modifying Analog Voice Card Channels

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- Viewing Analog Channel Identifiers

Modifying Analog Voice Card Properties

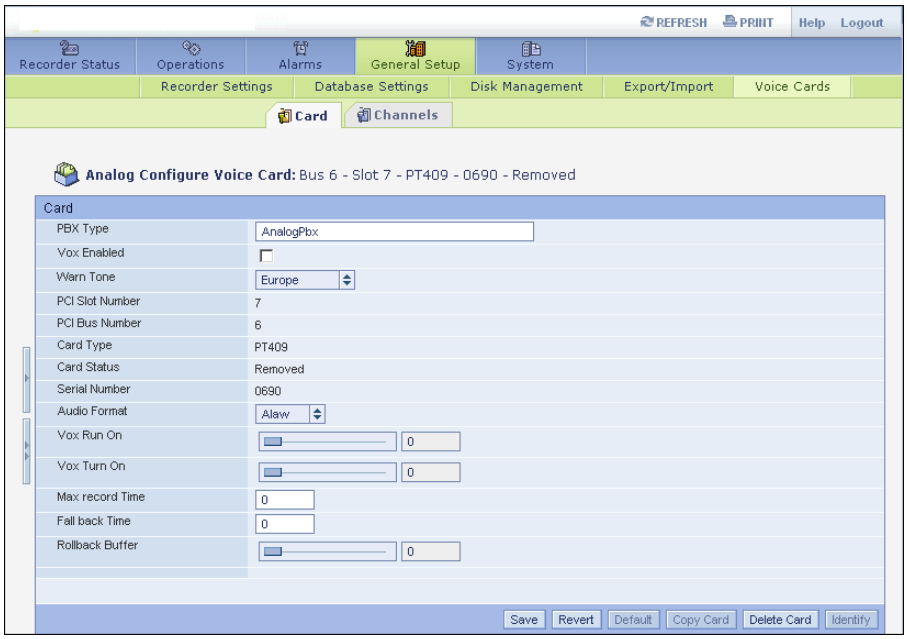
Modify an Analog voice card with a status of Existing to implement any analog card or channel configuration changes. To modify an Analog card, you select the card in the voice card list on the left pane then make changes and save the changes in the right pane. The new settings take place upon restart. You can also perform a number of actions including copying and identifying the card by clicking the action buttons.

To modify an analog voice card:

1 Choose **General Setup > Voice Cards > Card**.

2 In the voice card list (left pane), select voice cards with a status of **Existing**.

At any time you can click the arrows between panes to expand and hide windows.



3 Complete the Analog voice card window as follows:

Field	Description
PCI Bus Number	Bus Number. Read-only
PCI Slot Number	Slot Number. Read-only
Data Source	Choose from the list the Data Source such as a Phone switch, to which this card is associated.
Member Group	Choose from the list the Data Source Member Group to which this card belongs

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Card Type	Card Type (PT409, PT809, PT1609, LD409, LD809). Read-only
Serial Number	Alphanumeric entry. Read-only
Card Status	Voice card status (Newly Added, Replaced, Removed, Existing). Read-only
Compression Type/Audio Record Format	Defines the method for encoding the audio data in a WAV file. Predefined options are Alaw, uLaw, G726, G729A (the default). This field is editable and required.
VOX Run On (ms)	Defines the length of time in milliseconds sound needs to be below the threshold before the VOX method determines a call has ended. Threshold is configurable on each channel. This field is editable and required. See also Completing the VOX Tutorial on page 157
VOX Turn On (ms)	Defines the length of time in milliseconds sound needs to be above the threshold before the VOX method identifies a call. Threshold is configurable on each channel. This field is editable and required.
VOX Enabled	Describes whether the VOX method for call recording is enabled. Options are **True** and **False**. Default is **False**. Required updateable field
Max Record Time (sec)	Maximum record time in seconds for a single call segment. Default is 3600 seconds. This field is editable and required
Fall Back Time (sec)	Maximum elapsed time in seconds before the Recorder switches to **tap sense** mode if there is a loss of CTI feed. Default is zero seconds. This field is editable and required.
Rollback Buffer	A measure in milliseconds (0-1000) that allows the user to configure a number of milliseconds (default is 1000 milliseconds) to automatically capture voice for a period before the start record command comes in. This allows the Recorder to compensate for delays in CTI or Unify processing and automatically rollback the voice and start recording a brief amount of time before the actual start record request is received. Required
Warn Tone	Warn tone setting that will alert the listener on the call that the call is being recorded. Pre-defined selections are: Europe, US-Canada, Australia, and None. None will be the default.

4 Click **Channel** to configure the channels associated with this card, as described in Updating the Configuration of Voice Card Channels on page 118

5 Click **Save** when finished.

Modifying Analog Voice Card Channels

Modify analog channels where permitted (some fields are read only) to match system architecture requirements. Compatible analog voice cards appear in Compatible Voice Cards on page 242.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To modify analog channels:

1 Choose **General Setup > Voice Cards** and select an analog voice card.

2 Click **Channels** and review the fields as follows:

Field	Description
Enabled	Field that determines whether a channel has been selected for use. Selecting the checkbox subtracts a license channel from the "Available License" counter and vice versa when a channel is unchecked. **Note**: For cards with a status of **Newly Added**, all channels are checked (enabled) regardless of whether the channel is licensed.
Channel #	Number of the channel on the card, such as 1, 2, or 3. This is a read-only field
Channel ID	Logical channel ID that is used in the Unify mapping table to identify the Channel. This is a 6-digit serial number of the Recorder plus a 5-digit index number that is assigned by the web service. This is a read-only field.
VOX Detect Level	Defines the threshold used for VOX-based call detection. Units are in decibels. This is a required field.
CCE Control	Indicates if the voice card is controlled by the Command Control Engine (Unify). Options are **True** and **False**. **True** is the default. This is a required field.
Start On Tap	Indicates that recording begins as soon as tapping of the analog line begins. Options are **Always**, **Never**, and **In Fall Back**. Default is **In Fall Back**. This is a required field. See also Completing the VOX Tutorial on page 157.
Stop on Tap	Indicates that recording stops when the tapping of the analog line ends. Options are Always, Never, and In Fall Back. Default is In Fall Back. This is a required field.
Report Tap Events	Indicates whether start and stop events triggered from VOX or D-channel detection on the telephony card are passed to the Command Control Engine (Unify or Integration Framework). Options are **True** and **False**, default **True**. For systems where VOX or D-channel (including fallback) is not being used, this setting can be set to **False** to reduce the number of events that have to be processed by the Command Control Engine, thereby reducing the processing load on the system.
AGC (Auto Gain Control)	Enables an option on the voice card to automatically amplify the voice on the channel when necessary. Options are **True** or **False**. Default is **False**. This is a required field.
Digital Input Gain	Defines a level of amplification that can be used on weak channels. This is a numerical field that is updateable. This is a required field.

3 Select a channel and click **Configure**.

4 Follow procedures described in Updating the Configuration of Voice Card Channels on page 118.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Viewing Analog Channel Identifiers

The following information displays in the lower pane (Trunk pane) of the configure window when you configure an individual channel. These fields, also known as static tags, are configurable only on the individual card level. That is, identifiers apply to the selected card only.

Field	Description
Channel Name	User definable channel name (alphanumeric). Optional field
Extension	Extension number (numeric). Optional field. This field is autopopulated with the Extension configured with the station span in in Enteprise Manager (EM) Data Sources. You cannot edit this field if Recorder Manager is associated with EM.
Agent ID	Agent Identifier (Alphanumeric). Optional field.

Voice Card Troubleshooting

Problem	Solution
New settings are not being effective, even after clicking Save	Reboot computer, as all voice cards do not update configurations dynamically.
The voice card supports dynamic configuration but new settings are not effective immediately.	Make sure the Capture engine is up and running.
When Default Configuration is clicked, nothing gets changed.	Either you already have the default configuration, or the XML configuration file is not available. Copy the XML configuration file from the software that came with the card.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Problem	Solution
The Recorder is not detecting all of the Ai-Logix cards installed in the system.	To allow the Recorder to properly recognize all voice cards, the cards should be uninstalled from the Windows device manager and the system rebooted. Then the cards will be properly recognized and Windows will load the drivers appropriately. Finally, when the drivers are loaded normally during the MSI install, the firmware is automatically updated on the cards. If the problem described above is encountered then the firmware on the cards will not be automatically updated during the TDM Recorder (ITS IP Recorder) software installation. In this case the Ai-Logix utility, "SmartWF.exe /u" should be run after the corrective action is taken to automatically update the firmware on the cards.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Problem	Solution
The bus and slot numbers of voice cards are not displaying.	Click the toggle button arrow in the centre of the page. In maximized mode, the bus# and slot# display.
When recording with an NGX voice card and an Avaya switch (Station-side recording), the call sometimes is not stopped when the call is disconnected on an AVAYA phone.	This issue is observed in a free seating (licensing) scenario. Normally the Function Keys on Avaya phones are configured like this: Function Key 1 --> Line 1 (subreason LUCENT_GREEN_LIGHT) Function key 2 --> Line 2 (subreason LUCENT_GREEN_LIGHT_1) Function key 3 --> Log on (subreason LUCENT_GREEN_LIGHT_2) Function key 4 --> Auto-in (subreason LUCENT_GREEN_LIGHT_3) Function key 5 --> AUX (subreason LUCENT_GREEN_LIGHT_4) Function key 6 --> ASSISTANCE (subreason LUCENT_GREEN_LIGHT_5) Function key 7 --> Log-off (subreason LUCENT_GREEN_LIGHT_6) Recording starts when TDM capture receives the EVT_FUNCTION_LIGHT_ON with any of the above subreason value. And it is stopped when it gets the EVT_FUNCTION_LIGHT_OFF event with the subreason value same as the EVT_FUNCTION_LIGHT_ON event that triggered the recording. Now the configuration that should be made in **C:\Program Files\witness systems\contactstore\ TDMConfig.xml** would be as follows. (This is applicable if you want to use Function keys 1 and 2 to start / stop the call. This changes if you want to use a different key. <x:startevents> <x:event x:eventname="EVT_FUNCTION_LIGHT_ON"> <x:subreason>LUCENT_GREEN_LIGHT</x:subreason> </x:event> <x:event x:eventname="EVT_FUNCTION_LIGHT_ON"> <x:subreason>LUCENT_GREEN_LIGHT_1</x:subreason> </x:event> </x:startevents> <x:stopevents> <x:event x:eventname="EVT_FUNCTION_LIGHT_OFF"> <x:subreason>LUCENT_GREEN_LIGHT</x:subreason> </x:event> <x:event x:eventname="EVT_FUNCTION_LIGHT_OFF"> <x:subreason>LUCENT_GREEN_LIGHT_1</x:subreason> </x:event>

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Completing the Channel Assignment Tutorial

Complete this tutorial to reinforce your understanding of channel configuration. In this tutorial you are presented with a a number of facts relating to digital channel assignments, followed by examples that illustrate the facts.

What does the Channel ID Column represent?

The Channel ID column represents the media channel number. This represent the media channel identified in the recording request from Unify and is globally unique to a Recorder. Unify references the channel ID including the Recorder serial number when issuing commands to the Recorder through eWare2CC using the legacy MediaStore command syntax such as 'startchannel'. Unify references the channel by the media channel number only when using the CSCapture source DLL 'sendmessage' command to send commands to the Recorder, such as 'MC:10'.

What is the Channel Number?

The Channel # represents the channel number index on a particular card and is unique only on each card. This number is not used externally to the Recorder.

When are Channel IDs assigned?

Channel IDs are assigned to a card when the card is first saved. When the card is first saved, its status changes from 'Newly Added' to 'Existing'. Once a card is saved, the channel IDs are locked to that serial number and will not change except as identified in point #4 and #5 below.

How are Channel IDs assigned?

Channel IDs are assigned in a continuous manner based on the number of channels that will be active on the card when it is first saved. For example if the trunks on the card are configured for Robbed Bit or the protocol is set to none it will show 24 channels per trunk. If the card is configured for ISDN it will be 23 channels per trunk. For E1 trunks it will be 30 channels per trunk. If this configuration is later changed, the channel IDs for the configured card will be added or removed to reflect the new number of channels.

How are channels added when protocols are changed?

If channel IDs are to be added, for example changing an existing card from ISDN to Robbed Bit (going from 23 to 24 channels) and there is no room in the channel IDs for the Recorder to insert a new channel number, then the existing channel IDs for the changed card will be moved to the end of the channel IDs for the Recorder. This is shown in the examples below.

How do you configure channel IDs from Recorder Manager?

If the channel IDs are not configured as desired because of a protocol or configuration change, the cards can be deleted from the Recorder Manager. The Recorder must then

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

be restarted and the cards added again, after being auto-detected, to save the channel IDs in the desired order and configuration.

How is channel numbering started for new cards?

Any new cards added to a system start their channel ID numbering from the highest channel number in the system plus one.

How do you renumber channel IDs?

Channel IDs are renumbered or moved across a whole card at a time. Therefore, for dual trunk cards, the channels are renumbered across both trunks even if the protocol on one of the trunks changed.

What if there is no room on the channel ID listing for additional channels?

The same rules apply to changing the configuration of a card from E1 to T1 or T1 to E1; if channels are added and there is no room in the channel ID listing, the card will be renumbered to the end of the channel ID listing. If channels are removed then there will be allowable holes in the channel ID list.

How can you check channel IDs?

If the channel IDs are ever in doubt, they can be inspected and noted through the Recorder Manager Voice Card configuration screen or by using the channel database population wizard in Unify.

Example 1: Card Set 1 - Initial save:

Card #1-DP3209-Robbed Bit - Channel IDs 1-24

Card #2-DP3209-Robbed Bit - Channel IDs 25-48

Card #3-DP3209-Robbed Bit - Channel IDs 49-72

Example 2: Card Set 2 - Initial save:

Card #1-DP3209-ISDN - Channel IDs 1-23 (24 is reserved)

Card #2-DP3209-ISDN - Channel IDs 25-47 (48 is reserved)

Card #3-DP3209-ISDN - Channel IDs 49-71 (72 is reserved)

Example 3: After initial save, modify Card Set 1 from Robbedt Bit to ISDN:

Card #1-DP3209-ISDN - Channel IDs 1-23

Card #2-DP3209-ISDN - Channel IDs 25-47

Card #3-DP3209-ISDN - Channel IDs 49-71

As you can see, the last channel IDs for each d-channel were removed, the channel IDs assigned to the existing channels did not change. There are now holes in the logical channel ID listing (24 and 48) but it does not cause any harm and is as expected. The

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Unify mapping table should be updated to not try and record on channels 24, 48 and 72 because they no longer exist from the Recorder's perspective. If a record command comes in for these channel numbers, the Recorder will harmlessly return an error message stating no channel by that number.

Example 4: After initial save, Card #1 from Card Set 2 is changed from ISDN to Robbedt Bit:

Card #1-DP3209-Robbed Bit - Channel IDs 1-24

Card #2-DP3209-ISDN - Channel IDs 25-47

Card #3-DP3209-ISDN - Channel IDs 49-71

As you can see, channel id 24 is reused when the protocol is changed to Robbed Bit. The Unify mapping table should be updated to add channel 24.

Example 5: Starting with the result of Example 1, the configuration of Card #1 is changed to E1 Robbed Bit:

Card #1-DP3209- E1 Robbed Bit - Channel IDs 73-102

Card #2-DP3209- T1 Robbed Bit - Channel IDs 25-48

Card #3-DP3209- T1 Robbed Bit - Channel IDs 49-72

Example 6: Starting with the result at the end of Example 5, a new card is added and configured for T1 Robbed Bit.

After saving the card the channel IDs will result in the following:

Card #1-DP3209- E1 Robbed Bit - Channel IDs 73-102

Card #2-DP3209- T1 Robbed Bit - Channel IDs 25-48

Card #3-DP3209- T1 Robbed Bit - Channel IDs 49-72

Card #4-DP3209- T1 Robbed Bit - Channel IDs 103 - 126

As you can see, the newly added card is added to the end of the channel ID list starting with the highest existing channel ID on the system plus 1 (102+1=103). Since it is initially saved as Robbed Bit, it is saved with 24 channel IDs.

Completing the VOX Tutorial

This tutorial describes the use of VOX settings and Tap Sense settings.

What is VOX?

VOX is a telephony term for a sound measurement protocol that defines the length of time, usually in milliseconds, that sound needs to be above or below a specified threshold before the VOX method determines that a call has started or ended.

What events trigger VOX?

For the analog card you can configure the SEENAUDIO and ENDAUDIO events to come from either VOX or voltage (electrical impulses from the line). If the VOX checkbox is

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

clear these events are triggered by voltage. If the checkbox is checked, these events are triggered by VOX.

The StartOnTap and StopOnTap fields control whether recording will start or stop automatically when SEENAUDIO and ENDAUDIO events occur. If you set both of these to "Never" then the Recorder would produce these events so that Unify could use them but never actually begin or end recording based on them. This might be used in a dialer environment with nail-up calls when you cannot rely on the line voltage to tell you when to stop one call and begin a new one.

What happens if Unify is also used for events?

If you set StartOnTap and StopOnTap to Always, the Recorder will always stop and start when it detects the SEENAUDIO or ENDAUDIO events. You could use Unify for additional tagging in this scenario, but this is not recommended. If Unify also sends start and stop events, duplication and confusing calls can result. At a minimum, trace log messages stating that you cannot start a started channel or stop a stopped channel will result.

What happens when "In Fallback" is set?

You could set StartOnTap to Always and StopOnTap to Never if you had a CDR-based environment where you just get one event at the end of the call so you must use the SEENAUDIO event to begin recording.

If you set StartOnTap and StopOnTap to "In Fallback" then recording will start and stop based on SEENAUDIO and ENDAUDIO events only if the recording is in fallback mode.

The VOX Enabled check box determines what conditions produce SEENAUDIO and ENDAUDIO events. The StartOnTap and StopOnTap settings determine how the Recorder will react to those events.

Example: VOX Enabled

The SEENAUDIO and ENDAUDIO events will be determined for each type of card when the VOX Enabled field is set to CLEAR as in the following examples:

- LD & PT Card (Analog): Line Voltage
- NGX Card (Digital Extension): Extension D-Channel events (usually lamp events, varies by switch type)
- DP Card + NONE, CAS, or RBS Protocol (Trunk Tap): ABCD Signalling bits
- DP Card + ISDN Protocol (Trunk Tap): ISDN D-Channel events

When the VOX Enabled field is checked, VOX will be used regardless of the card type. This means that SEENAUDIO is determined when a sound is louder than the VOX Detect Level for a period of time equal to or greater than the VOX Turn On time. ENDAUDIO is determined when the sound drops below the VOX Detect Level for a period of time equal to or greater than the VOX Run On time.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Network Interface Cards

Configuration of network interface cards (NICs) for IP recording describes the process of setting up network cards, filters and protocols. Detection of standard NICs for IP recording is an automatic process. After installing the NIC by following standard safety procedures for installing a card into a PC, the Windows operating system automatically detects the new hardware and configures accordingly.

Information is presented in the following section:

- Configuring Network Settings

Configuring Network Settings

Configure IP network settings to setup network interface cards (NICs) and filters, and to assign communication protocols for telephones and devices (specifically the Remote Analyzer). Network settings determine the amount of traffic that must be processed, a task that is streamlined by the network filters you specify. Recorder Manager simplifies the task by presenting a list of NICs and a list of supported protocols. This information is described in the following topics:

- Configuring Network Cards and Filters
- Configuring Network Protocols

Configuring Network Cards and Filters

Configure cards and filters to reduce the amount of traffic that IP Recorders and IP Analyzers need to monitor. Filters serve multiple purposes:

- Protect the Recorder from receiving excessive, unneeded packets.
- Repress packets that the Recorder potentially does not understand.
- Remove specific IP address ranges and traffic.
- Remove duplicate packets if configured at a per NIC level.

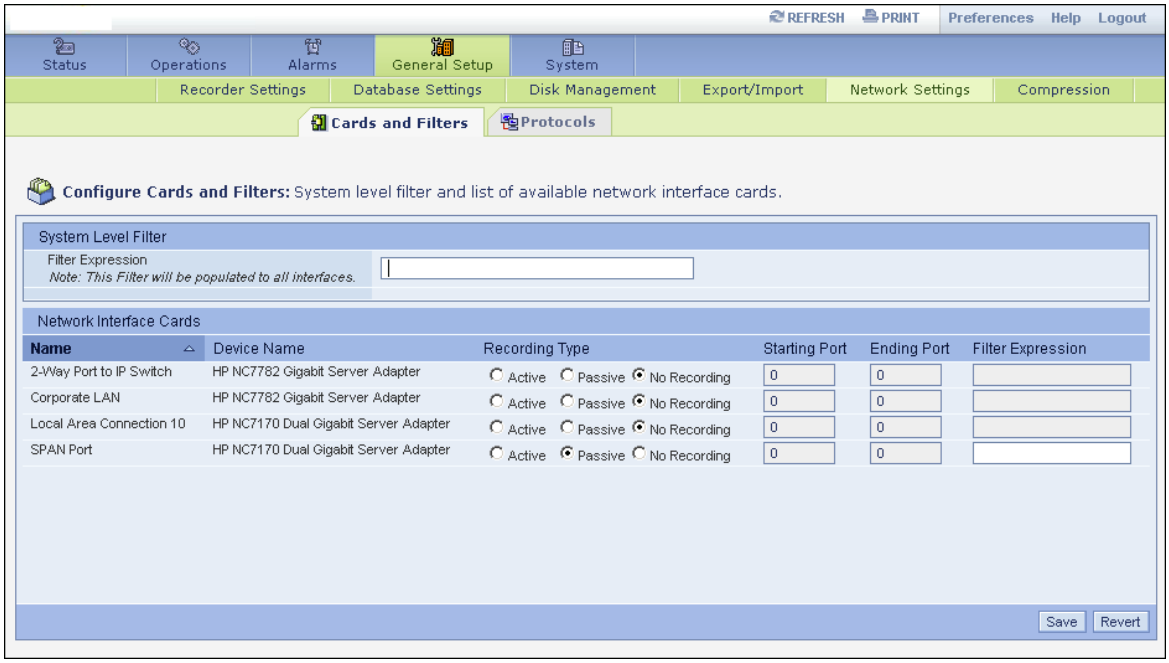
You can also configure the NIC(s) in some TDM Recorders (ITS IP Recorders) to create settings needed by the IP emulation of pseudo wire emulation protocols (PWE3).

To configure network cards and filters on an IP Recorder:

Configure network cards and filters on an IP Recorder to filter IP traffic. Reduced traffic means increased performance because by filtering network traffic to allow only IP packets that meet conditions specified in the filter, unnecessary traffic is reduced or eliminated. Before completing this area, you need to obtain filter expressions from your system architect or by visiting http://winpcap.com for filter expressions.

1 In an IP Recorder, choose **General Setup > Network Settings > Cards and Filters**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Complete the Cards and Filters window according to the following:

Item	Description
System Level Filter	Heading for entering system level filters. Read only field.
Filter Expression	Type a filter expression for the System level filter. This filter is applied to all expression interfaces. For example, an expression such as TCP 2000 (an algorithm) acts as an IP filter to screen all IP traffic moving between components. You can apply filters at two levels from Recorder Manager: the system level, and combined with the network interface card (NIC) filter. If a Recorder has more than one NIC, a system-level filter applies to all of them. See also on page 165 below.
Network Interface Cards	Heading for list of NICs. Read only field.
Name	Shows a read-only description of the Network Interface Card.
Device Name	Shows the read-only network connection name associated with the NIC.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Item	Description
Recording Type	Choose an option for recording type from **Active, Passive**, and **None**. When you choose **Active**, the Starting Port and Ending Port fields are enabled and Filter Expression disabled, allowing recording of data from the specified starting and ending ports regardless of filter expression. When you choose **Passive**, Starting Port and Ending Port are disabled, and Filter Expression enabled, allowing selective recording based on the filter expression. When you choose **None**, Starting Port, Ending Port and Filter Expression are disabled and no recording takes place. Default value for recording type is **Passive**.
Starting Port	Starting port specific to the Protocol. Only numerals separated by a comma are acceptable. The value should be less than the Ending Port, This field is enabled only if the Active recording type is selected.
Ending Port	Ending port specific to the Protocol. Only numerals separated by a comma are acceptable. The value should be greater than the Ending Port, This field is enabled only if the Active recording type is selected.
Filter Expression	Shows the name of the protocol or just protocols that are specific to the card. This is an expression such as TCP (transmission control protocol). The value is also the filter expression being used for this NIC.The actual filter expression is the logical sum (that is, the operator AND) of the filter on each card and the filter specified at the system level. See also on page 165 below.

3 Click **Save**.

Filter Expression Examples for RTP-based IP Recorders

You can reduce the amount of traffic that IP Recorders and Analyzers need to monitor by creating and applying network filters. A filter screens network traffic, allowing through only traffic that meets the conditions specified in the filter. Since a well-constructed filter can reduce or eliminate unnecessary traffic, it can improve your system performance.

You can apply filters at two levels — the system level, and the Network Interface Card (NIC) level. If a recorder has more than one NIC, a system-level filter will apply to all of them. If you also apply NIC-level filters, the system appends these to the system-level filter. (Make certain that your system-level and NIC-level filters do not contradict or otherwise interfere with each other.) The Recorder uses WinPcap for network filtering. You can find information on their standardized filter syntax online, at http://www.winpcap.org. For detailed information on syntax, refer to http://www.mirrors.wiretapped.net/security/packet-capture/winpcap/docs/docs31/html/group__language.html.

The most typical filters would be:

`tcp port 2000` or **`udp`**. This filter should be used in a standard Cisco SCCP environment. It tells the driver to let packets of port 2000 through; these are the SCCP packets, and also to let UDP packets through, which contain the RTP and therefore the audio.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

`tcp port 5060` or **`udp`**. This filter should be used in standard SIP environments. This filter lets the SIP control protocol through on port 5060 as well as the UDP, which contains the RTP and therefore the audio.

At a minimum, you should use the following standard pcap filters:

For Recorders that use SIP: **(tcp port 2000 or tcp port 5060) or (udp and not udp port 0).** This filter lets the SIP control protocol through on ports 2000 and 5060 as well as the UDP, which contains the RTP and therefore the audio.

For Recorders that do no use SIP: **tcp port 2000 or (udp and not udp port 0)**

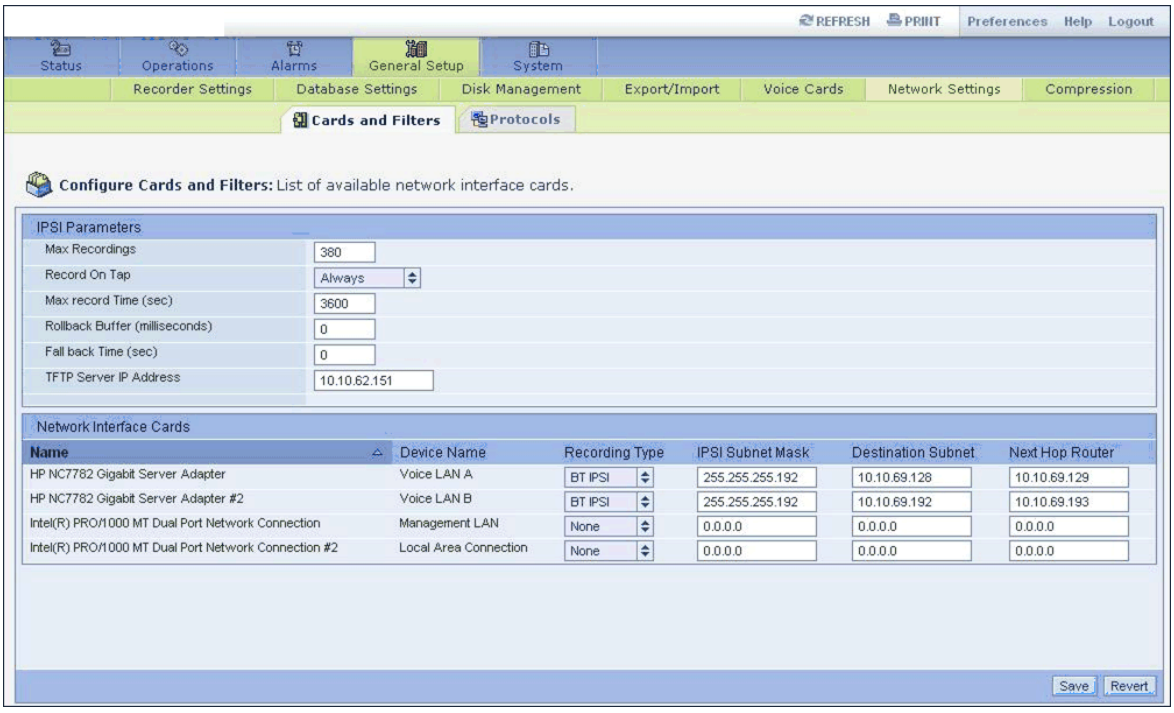
Because port numbers change according to customer environment, you should check with your system architect that the above port numbers correctly reflect your environment.

For more information, you can also Google the term **winpcap filters**.

To configure IPSI network cards and filters on a TDM Recorder (ITS IP Recorder):

Configure IPSI network cards and filters only to configure IP recording in an ITS Link environment. TDM recording does not require the **Cards and Filters** page to be completed.

1 In a TDM Recorder (ITS IP Recorder), choose **General Setup > Network Settings > Cards and Filters**.



© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

2 Complete the Configure Cards and Filters window according to the following:

Item	Description
IPSI Parameters	**Heading for IP Switch Interface (IPSI) settings only.**
Max. Recordings	Type the maximum number of channels that can be recorded with this card. This value is typically a multiple of 32.
Record On Tap	Choose **Always** as the record on tap option. Other options include **Always, Never,** and **In Fallback**. These define when the Recorder is to record calls using tap sense when other Recording Control Types fail. Default is **Always**. With the **Always** setting, the Recorder always records on tap when necessary. With the **Never** setting, the Recorder never records on tap. With the **In Fallback** setting, the Recorder records using tap sense only when in In Fallback (backup) mode.
Max. Record Time (Sec)	Shows the maximum time in seconds that the call can be recorded before starting to record on a new **`inum`**. Default time is 3600 seconds (60 minutes). This field is optional.
Rollback Buffer (milliseconds)	Shows a value measured in milliseconds (0-1,000) that allows you to configure a number of milliseconds (default is 1,000) to automatically capture voice for a period before the start record command comes in. Recommended setting is 250 ms. This allows the Recorder to compensate for delays in CTI or Unify processing and automatically rollback the voice and start recording for a brief amount of time before the actual start record request is received.
Fallback time (Sec)	This field does not apply, as only tap-sense based recording is performed. Normally, this setting refers to the maximum elapsed time in seconds before the Recorder switches to **tap sense** mode if there is a loss of CTI feed. Default is zero seconds.
TFTP Server IP address	The global_ipconfig.txt file is essential to the operation of the ITS. It contains the IP addressing information for all of the ITS components. All ITS components load this file from the system Trivial File Transfer Protocol (TFTP) area during the first start up steps. The global_ipconfig.txt file must reside in the TFTP directory on the ITS Admin server. The TDM (IP) Voice Recorder expects to find the following records defined in this file: • **`IPSIVoicePortNum=xxx.xxx.xxx.xxx`** • **`IPSIHeartbeatPortNum=nnnn`**
NICs	**Heading for list of Network Interface Cards (NICs).**
Name	Shows a read-only description of the Network Interface Card.
Device Name	Shows the read-only network connection name associated with the NIC.
Recording Type	Choose an option for recording type from **BT IPSI**, (the British Telecom IP switch interface that supports the recording of trading turrets) and **None**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Item	Description
IPSI Subnet Mask	Type the IP address of the IPSI subnet mask. The subnet mask is used to determine what subnet an IP address belongs to. An IP address has two components: the network address, and the host (workstation) address. For example, consider the IP address 150.215.017.009. The first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host (workstation) on this network.
Destination Subnet	Type the IP address of the host (workstation) address, as described in IPSI Subnet Mask above.
Next Hop Router	Type the IP address of the next logical router device in the network.
Routes Required for IP connection of VR to IPSI	Two routes to the IPSI subnets must be carefully added to the voice recorders' routing table. These are added by entering the properties in the RM configuration, saving the data and restarting the Recorder TDM Capture engine service. The two route formats are: **`route add <subnetA> MASK <netmaskA> <gatewayA>`** **`route add <subnetB> MASK <netmaskB> <gatewayB>`** For example: If NIC Voice LAN A has an IP address of 10.221.47.121, and Voice LAN B has an address of 10.221.47.251, then: **`route add 10.221.45.0 MASK 255.255.255.128 10.221.47.126`** **`route add 10.221.46.0 MASK 255.255.255.128 10.221.47.254`** where: • **`subnetA`** is the unique subnet for Voice LAN A on the IPSIs • **`subnetB`** is the unique subnet for Voice LAN B on the IPSIs • **`netmaskA/B`** is the netmask for the Voice LAN A/B in the IPSIs • **`gatewayA/B`** is the "next hop" router for Voice LAN A/B from the voice recorder **Notes:** a. Persistent routes could be used, but these routes must be deleted whenever the routing information changes. If non-persistent routes are used, remember that they must be added to the routing table after the voice recorder has been rebooted and prior to starting the heartbeat service. b. Batch files could be created and used for ease of adding and deleting these routes. c. N.B. No default gateway should be set, only **Next Hop Router** should be set.

3 Click **Save**.

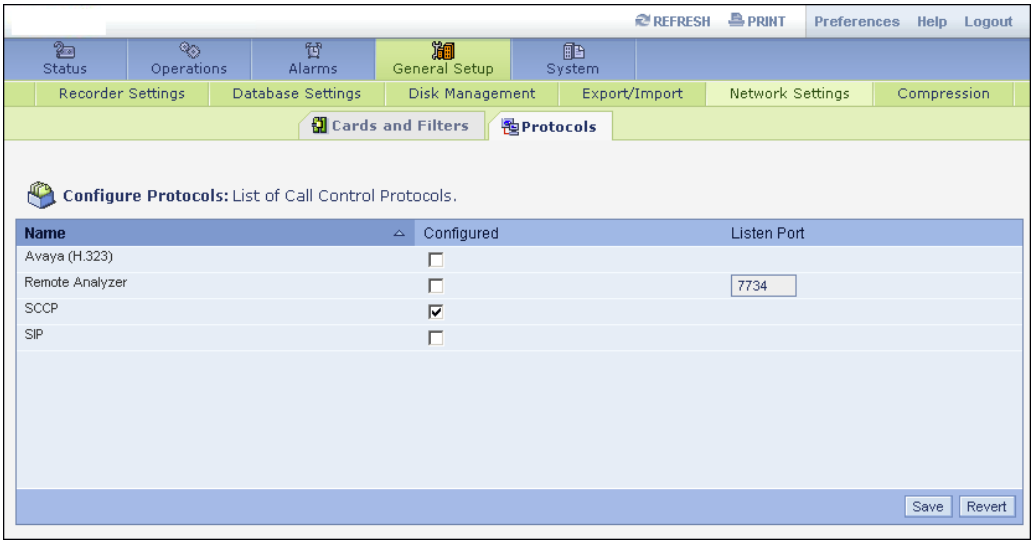
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Network Protocols

Configure call control protocols in the network to identify which IP communication protocol is used for Recorder Controlled extension management, including Analyzer if installed. Either one of two common protocols can be configured, SCCP and SIP. The Remote Analyzer protocol can also be used. If your Extension Recorder Control Type is CTI Controlled or Unify controlled, do not configure SCCP or SIP, as these will trigger recordings and over-ride existing CTI- or Unify Controlled settings.

To configure network protocols:

1 Choose **General Setup > Network Settings > Protocols**. The Protocols window displays, according to your selection of NICs in the Cards and Filters window.



© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

2 Complete the Protocol window according to the following:

Item	Description
Name	Shows the name of the protocol. **Avaya (H.323)** is a common multimedia communications protocol used in packet-based networks. **Remote Analyzer** is the name of the proprietary protocol used for call control. **SCCP** (Skinny Call Control Protocol) is used with either Cisco IP phones or Cisco Call Managers. **SIP** (Session Initiated Protocol) is a common IETF non-proprietary call control protocol.
Configured	Check a protocol (Avaya H.323, SIP or SCCP) to be used if the Extension Recorder Control Type is **Recorder Controlled**. If the Extension Recorder Control Type is NOT **Recorder Controlled** (that is, extensions are CTI Controlled or Unify Controlled), leave these fields unchecked. If you check Remote Analyzer as the protocol, you must also type in a port number under **Listen Port**.
Listen Port	Only if **Remote Analyzer** is checked, type the number of the port on which the Recorder *listens* to (that is, communicates with) the Analyzer. The Port field is available only for the Remote Analyzer protocol. The port number specified should match the port in the Analyzer Call Control Protocol configuration as described in Creating a Call Control Recorder Group on page 179.

3 Click **Save**.

Tutorial: Configuring Call Manager for Active Recording:

This tutorial describes how to set up Cisco's Call Manager 6 (CCM6) to record calls using Active Recording. It is assumed that CCM6, Enterprise Manager, and Recorder Manager have been installed correctly. Information is described in the following topics:

- Setting up the Call Manager
- Setting up Enterprise Manager
- Setting up Recorder Manager

Setting up the Call Manager

You or your Cisco system administrator can set up Call Manager to perform active recording by configuring the Call Manager Administration application. Configuring Call Manager is beyond the scope of this guide but is included for completeness. For more information, refer to the appropriate Cisco documentation.

To set up the Call Manager:

1 Launch the Call Manager Administration application and create a SIP Trunk by doing this:

- Log on to Call Manager 6 and choose **Device > Trunk > Add New**.
- Select **Trunk Type > SIP Trunk**, and then click **Next**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- Complete the other fields as follows:
  - Type a name for the SIP trunk.
  - For **Device Pool** select **Default**.
  - For **Destination Address** type the IP address of the Recorder.
  - Make sure **Destination Port** matches Recorder settings.
  - For **SIP Trunk Security Profile** select **Non-secure**.
  - For **SIP Profile** select **Standard Profile**.
- Click **Save**.

2 Create the **Recording Profile** by doing this:

- Select **Device > Device Settings > Recording Profile-> Add New**.
- Enter the name of your recording profile.
- For **Recording Destination Address** enter the phone extensions of the SIP trunk (configured when you created the route pattern).
- Click **Save**.

3 Configure **Phone** settings and **Line Appearance** settings by doing this:

- For each phone you need to configure for active recording:
- Select **Device > Phone > Find**.
- Select an extension from the list (click the device name).
- For **Built In Bridge** select **On**.
- For **Privacy** select **Off**.
- Click **Save**.
- Click the line appearance (upper left-hand part of screen) and on the line appearance page, do this:
- For **Recording Option** select **Automatic Call Recording Enabled**.
- For **Recording Profile** select your recording profile (from the previous step).
- Click **Save**.
- Reset the phone by clicking the reset button then clicking **Reset**.

Setting up Enterprise Manager

Set up Enterprise Manager (EM) to create the Recorder within the enterprise and associate it with the Call Manager switch (that is, the Data Source). You also set up a Member Group to create extensions and associate them with the Data Source. Detailed procedures appear in the *Enterprise Manager Administration Guide.*

To set up Enterprise Manager:

1 Launch EM, choose **System > Installations,** and with your Site selected, click **Create Installation > Server**, and then add the Recorder server to your site. This is described in *Creating Installations*.

2 Click **System > Administration > EM Location > Update Recorders.** This registers the Recorder in the network and allows it to be controlled by EM.

3 Register the Call Manager as the Data Source, as described in *Creating a Data Source*:

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- Click **System > Data Sources,** and then create a Data Source of type **Phone.**
- Choose **Cisco IP** as the switch type, and accept default values for all other fields.

The Data Source is now created.

4 Create extensions, as described in *Setting up Telephony Groups (Member Groups)*:

- Click **System > Data Sources > Member Group,** and then select the Call Manager Data Source you just created.
- Click **Create,** and then choose **IP Extension Pool** as the Member Group type. This is described in *Setting up IP Extension Pools*.
- Choose **External Controlled** as the Recorder Control Type, as described in *Creating and Editing Phones*.
- Click **Manage Extensions,** and then assign extensions as described in *Managing Extensions in an IP Extension Pool Group*, and *Assigning and Unassigning Extensions*.

5 Click **Manage Recorder Association**. This links the Call Manager with the Recorder server you created earler so that the Call Manager communicates only with this Recorder. This is described in *Associating Recorders*.

6 Click **Save** and close EM

Setting up Recorder Manager

Set up Recorder Manager (RM) to complete the Active Recording 'point and click' configuration. This is basically a three-step process where you: 1. Create a SIP Adapter, 2. Link the Adapter to the Call Manager Data Source that you created in Enterprise Manager, and 3. Click the Active Recording radio button on the NIC.

To set up the Recorder:

1 Log on to RM and add the SIP Adapter by doing this:

- Click **System > Integration Framework**
- Choose **SipProxyAdapter** as the Adapter Type.
- Associate the Call Manager, as set up in EM, and include the Port and Protocol you created.

2 Link the Adapter to the Call Manager by copying settings for the Adapter as follows:

- Open **`IFService.xml`** located under the **c:\Program Files\Witness Systems\conf** folder.
- Move the <**Integration**> node of type **SipProxyAdapter** under the <**Integrations**> node to the integrations node for **`RecorderController.xml`**. This associates the Adapter with the Recorder when saved.
- **Save,** and then close both files.
- Restart the **Integration Framework** and **Recorder Controller** service.

3 Configure IPCapture as follows:

- In RM, select **General Setup > Network Settings > Card and Filters**
- Beside a NIC select **Active** as the Recording Type.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- Indicate the ports to be used for recording. For example, the Start Port could be **9200** and the End Port could be **9219**. Each concurrent active recording takes 2 ports
- Restart the **IP Capture** service

4 Verify the association by referring to sytem logs:

- Run **C:\Program Files\Witness Systems\ContactStore\LogManager.exe**
- Choose **RecorderController**
- Paste the directory value into the directory and change the trace level to **Debug High**
- Click **Apply**
- Repeat the same steps for **IntegrationFramework** and **IPCapture**.
- Choose **Save**, and then close the application
- Restart the system

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Analyzer

Configure Call Control in Analyzer to add and edit Recorder groups. Call control is available only if analyzer is installed. Analyzers analyze the call control messages (that is, the metadata about a call) and send call control commands, using the Remote Analyzer Protocol, to Recorders in a Recorder group associated with the voice gateway through which calls pass.

The Analyzer Manager user interface is identical in many places to Recorder Manager except that Analyzer does not have any local archive,compressor, disk manager, or database manager. Analyzer, therefore reports no performance statistics in these areas.

The Anaylzer is used to span control traffic in a remote location to the Recorders such that it can provide call control data (i.e. call metadata) that the Recorders would not see otherwise. This process enables Recorders to record audio from one area of the network and the call control protocol from a different area.

Analyzer configuration information is presented in the following topics:

- Viewing Analyzer
- Using Analyzer Manager
- Configuring Call Control

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Viewing Analyzer

View management features in the optional Analyzer component by logging in to it, and then reviewing the Analyzer's status. This information is described in the following topics:

- Viewing Analyzer
- Using Analyzer Manager
- Configuring Call Control

Accessing the Analyzer

Access the Analyzer, providing you have security authorization, by logging in. Analyzer Manager resembles Recorder Manager, only with fewer tabs. For example, there is no Database Settings or Disk Management tabs as Analyzer does not have these features.

To access the Analyzer:

1. In the Analyzer Manager server, click **Start > Programs > Witness > Recorder Manager** or click a desktop shortcut.
2. Log in to the Analyzer Manager by entering the default username *superuser* and password *WitPa&&word1*, or any other assigned.
3. Create users as described in Adding Users on page 28.

Viewing the Analyzer Status

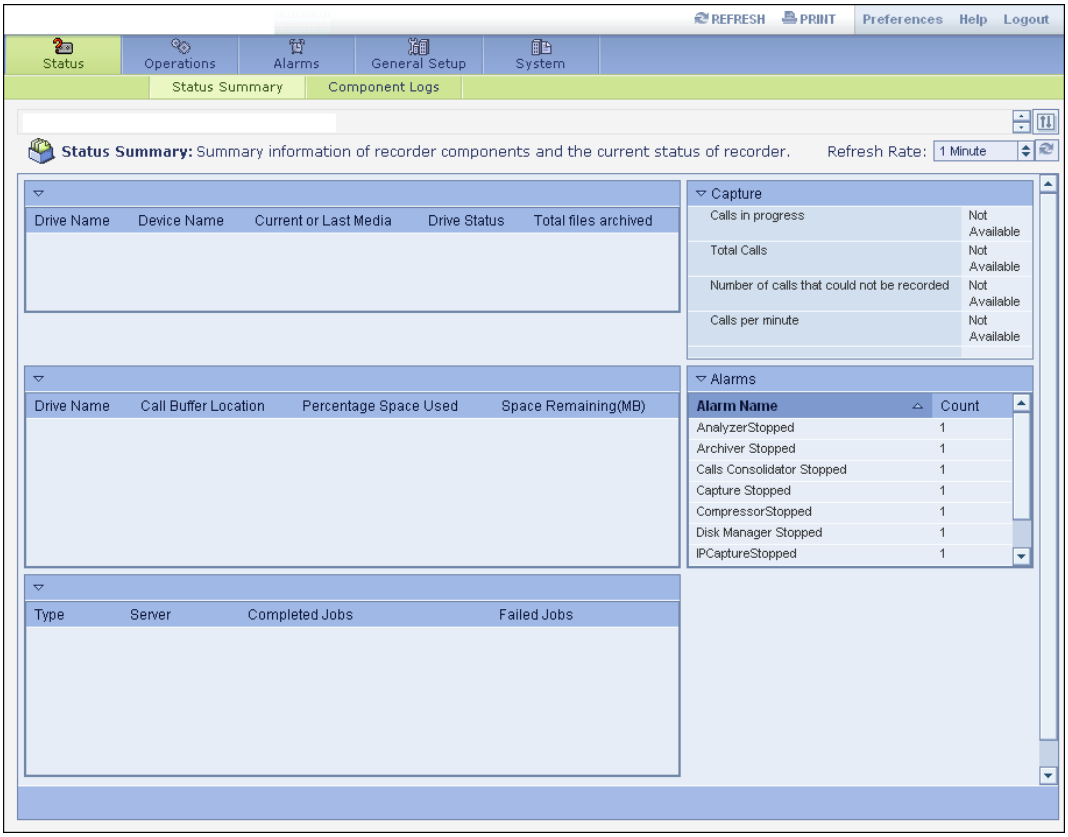
View the status of the Analyzer, similar to the Recorder Status page, to view a summary of activities of all the working components. The Analyzer status page can be set to display automatically, as set up in the Preferences file, or it can be launched from Analyzer Manager.

To view the Analyzer status:

1. Log in to Analyzer Manager as described in Accessing the Analyzer on page 171.
2. Do one of the following:

- Review the Analyzer Status page if it appears automatically. For field descriptions, refer to Viewing the Analyzer Status on page 171.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



- If the Alarms page displays at startup, click **Status > Status Summary.** To set the Status Summary page to appear automatically at startup in future, follow procedures in To view the Status Summary page automatically on start up: on page 172 (below).

To view the Status Summary page automatically on start up:

You have two choices for the initial screen, namely Status Summary (the default) and View Alarms. Follow this procedure to always view a Status Summary at startup.

1 In Analyzer Manager, click **Preferences** on the menu bar of any screen.

2 For **Default Screen at Login**, choose **Status Summary**. You would choose View Alarms to view alarms automatically at startup.

3 Click **Save**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Using Analyzer Manager

Use Analyzer Manager to perform analyzer management functions that enable Analyzer, an optional component in the recording system, to integrate with the IP Recorder. This includes all the familiar tasks you can perform in Recorder Manager, such as managing alarms and users, except that all tasks relate only to the Analyzer. You cannot create or update licenses from Analyzer. In addition, if your recording system is controlled by an Enterprise Manager, permissions can be assigned to the Analyzer, which is another form of an Installation (Search and Replay and Recorder being the other types), limiting who can access this application. You must therefore have the requisite security authorization to access Analyzer.

Analyzer information is described in the following topics:

- Working with Analyzer Component Logs
- Starting and Stopping Analyzer Services
- Managing Analyzer Alarms
- Performing Analyzer General Setup
- Setting up Analyzer Logs
- Connecting Analyzer to an Email Server
- Managing Analyzer Users
- Setting up Analyzer Preferences

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Working with Analyzer Component Logs

Access Analyzer's component logs to view and manage the various component logs. In this window, you identify Analyzer components being logged, set date ranges, and export or clear the logs.

To export or clear component logs:

1. In the Analyzer server, start Analyzer Manager and click **Status > Component Logs**.
2. In the list of Components, select **Alarms**, **Capture** and **Live Monitor** (if installed).

   Archiver, Calls Consolidator, and Disk Manager components cannot have component logs as these components are not present on the Analyzer.
3. Follow procedures described in Exporting and Clearing Component Logs on page 208.

Starting and Stopping Analyzer Services

Manage the services of Analyzer components by starting and stopping them in a controlled manner from Analyzer Manager.

To start and stop Analyzer components:

1. In the Analyzer server, start Analyzer Manager and click **Operations > Start and Stop**.
2. Follow procedures described in Starting and Stopping the Recorder and Components on page 59.

Managing Analyzer Alarms

Manage alarms in Analyzer in a similar fashion, though on a smaller scale, to Recorder Manager. As with Recorder Manager, you can configure parties to be notified when Analyzer alarms are triggered and you can type Alarm settings and history properties.

To manage analyzer alarms:

1. In the Analyzer server, start Analyzer Manager and click **Alarms**.
2. Follow procedures to view alarms, set alarm notification profiles, and type alarm settings as described in Monitoring Components with Alarms on page 184.

Performing Analyzer General Setup

Use Analyzer's general setup features to view Analyzer settings, save and export the analyzer's configuration file, import files from other sources, and type call control and network settings. There is no option for card settings as the Analyzer processes IP traffic only using a network interface card.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To view Analyzer settings:

Use Analyzer settings to confirm the System Type and verify the server name.

1. In the Analyzer server, start Analyzer Manager and click **General Setup > Recorder Settings**.
2. Follow procedures described in Starting and Stopping the Recorder and Components on page 59.

To export the Analyzer configuration file:

1. In the Analyzer server, start Analyzer Manager and click **General Setup > Export/Import**.
2. Follow procedures described in Exporting Configuration Information on page 206.

   The Analyzer's configuration file is exported according to launch type: if you are accessing the export functionality from Recorder Manager, the configuration file is exported as a consolidation of configurations of all components. If you are accessing the Analyzer from Enterprise Manager, you can export individual component configurations.

To import files into Analyzer:

1. In the Analyzer server, start Analyzer Manager and click **General Setup > Export/Import**.
2. Follow procedures described in Importing and Restoring the Configuration File on page 207.

   The Analyzer's configuration file is imported according to the method in which this file was exported.

To add Analyzer Recorder groups and IP addresses:

Add Recorder groups and IP addresses using Analyzer Manager to identify groups of Recorders within the network, to indicate the IP Gateway switch that supplies IP traffic to the group, and to type the IP addresses of the Recorders within the group.

1. In the Analyzer server, start Analyzer Manager and click **General Setup > Call Control**.
2. Follow procedures as described in Configuring Call Control on page 177.

To create Analyzer network settings:

Add Recorder groups and IP addresses using Analyzer Manager to identify groups of Recorders within the network, to indicate the IP Gateway switch that supplies IP traffic to the group, and to type the IP addresses of the Recorders within the group.

1. In the Analyzer server, start Analyzer Manager and click **General Setup > Network Settings**.
2. Follow procedures as described in Configuring Network Settings on page 159.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Setting up Analyzer Logs

Set up Analyzer logs to customize and view log configurations and manage log files by activating them. Log files can be invaluable in troubleshooting system problems.

To set up Analyzer logs:

1. In the Analyzer server, start Analyzer Manager and click **System > Log**.
2. Follow procedures as described in Using System Logs on page 30.

Connecting Analyzer to an Email Server

Connect Analyzer to an email server so that alarms triggered in the Analyzer can be notified using email's SMTP and the data network's SNMP, to Recorder Manager and Enterprise Manager if present.

To connect Analyzer to an email server:

1. In the Analyzer server, start Analyzer Manager and click **System > Email Server**.
2. Follow procedures as described in Configuring E-mail Servers on page 200.

Managing Analyzer Users

Manage Analyzer users to create new users, edit existing ones, and to create or change passwords for existing users of the Analyzer.

To manage Analyzer users:

1. In the Analyzer server, start Analyzer Manager and click **System > Manage User**.
2. Select a user and then follow procedures as described in Creating Users on page 27.

Setting up Analyzer Preferences

Set up Analyzer preferences to set defaults for general and user interface preferences. For example, you can set time formats and specify a preference for the first window to appear when the Analyzer Manager is first started.

To set up Analyzer preferences:

1. In the Analyzer server, start Analyzer Manager and click **Preferences** in the menu bar of any window. The preferences you select here will apply to all users of the Analyzer Manager. However if the Analyzer is accessed from Enterprise Manager, the preferences from Enterprise Manager override Analyzer Manager's preferences.
2. Follow procedures as described in Using Help on page 35.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Call Control

Configure Call Control in Analyzer to set up call control parameters so that the call control messages for IP calls are routed to the Recorders associated with the voice gateways where the calls will go through. Call Control is available only if an Analyzer is installed. Analyzer forwards SCCP, based upon the IP address of the gateway, to the Recorder specified by its IP address.

Before configuring Call Control, you should have a network diagram showing all Gateway IP addresses and Server names and Ports.

Information is presented in the following topics:

- Viewing Call Control Information
- Creating a Call Control Recorder Group
- Editing a Call Control Recorder Group

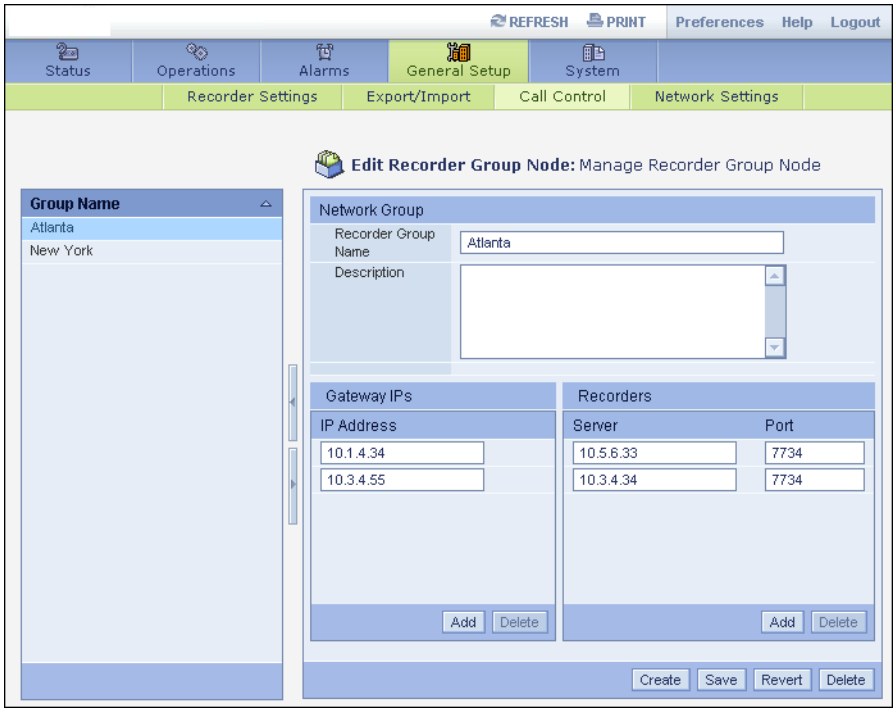
Viewing Call Control Information

View call control information in Analyzer Manager to obtain a summary of recording groups and Gateways in your IP recording environment. You can also view details of each Recorder group, which includes IP Addresses of the targeted Gateway, and IP addresses of the Recorders in the group.

To view call control information:

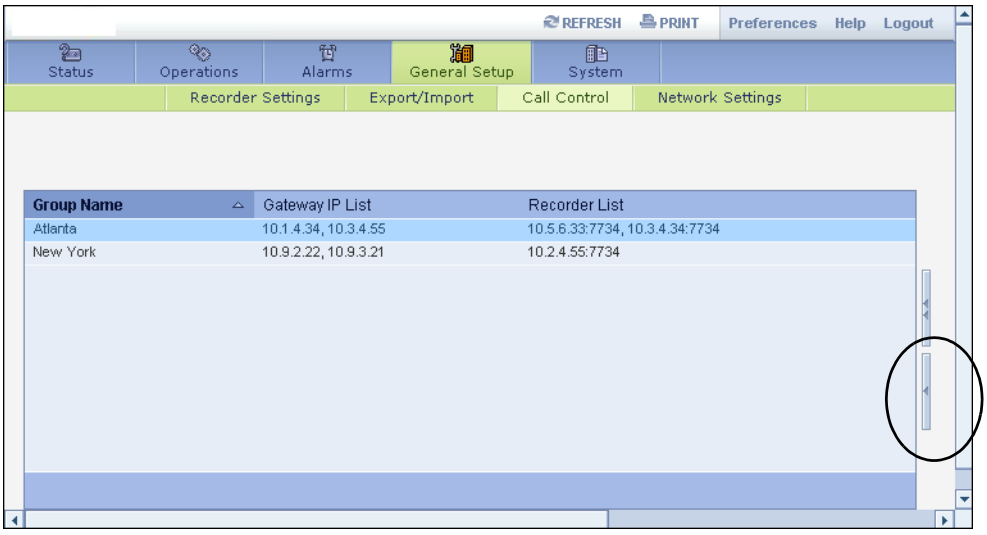
1 In Analyzer Manager click **General Setup > Call Control**. The Call Control window displays all Groups.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Click the right-pointing arrow that separates the two panes. This provides a detailed view of Recorder group list.

Click the left-pointing arrow to display the Group/Gateway/IP details pane alone.



3 Click a group to display editable details of that group, as described in Creating a Call Control Recorder Group on page 179 and Editing a Call Control Recorder Group on page 180.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

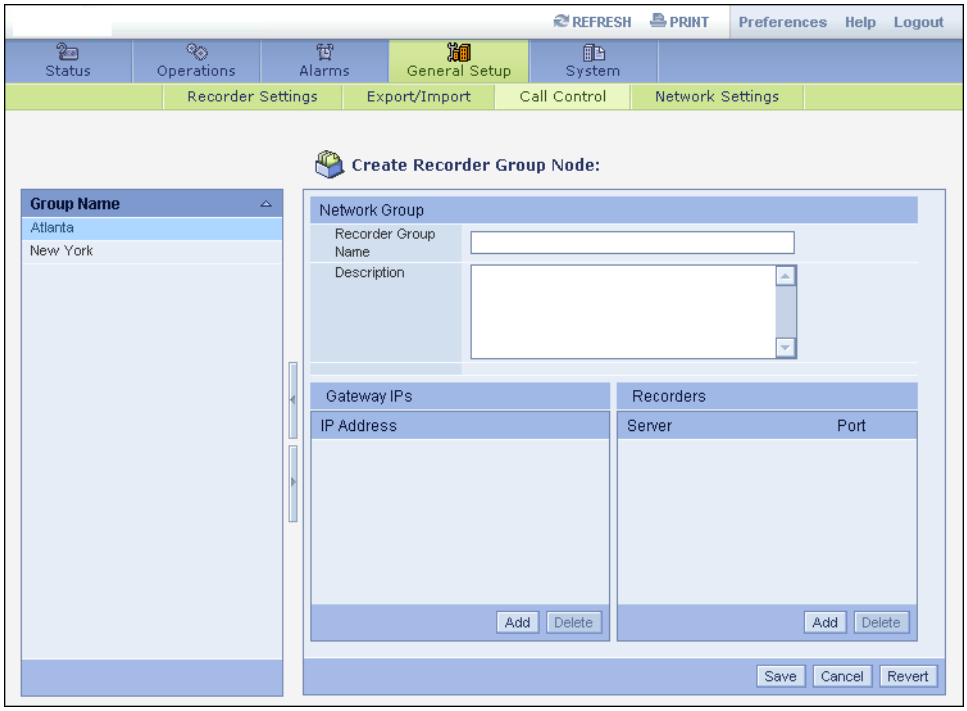
Creating a Call Control Recorder Group

Create a Call Control Recorder Group to identify gateway IP addresses and Recorders that are associated with the recording of IP calls within the group.

To create a Recorder group:

1 In Analyzer Manager click **General Setup > Call Control**. The Call Control window displays.

2 Click **Create**. The Create Recorder Group window displays.



3 Complete the Recorder Group window fields as follows:

Item	Description
Recorder Group	Shows details of the Recorder group (read only field).
Recorder Group Name	Type a name for the Recorder group.
Description	Type a description (optional) of the Recorder group.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Item	Description
Gateway IPs	Type the IP address of the Gateway whose SCCP-related traffic you want forwarded to the remote Recorder, as in the following example: `10.3.4.5`. Click **Add** after each entry to create a new line that will accept a new IP address. The Gateway is the endpoint that the Recorder Group will see RTP traffic for. To delete Gateway information, highlight it after clicking Add and then click **Delete**.
Recorders	Type the IP address of the Recorder that is to receive that Gateway's SCCP, along with the port number, as in the following example: `10.3.5.62:3030`. Click **Add** after each entry to create a new line that will accept new information. **Note**: The port number must be a numeric value between 1024 and 65355. To delete Recorder information, select the Recorder's details after clicking Add and then click **Delete**.

4 Click **Save**

The Recorder group is added to the Group Name pane on the left.

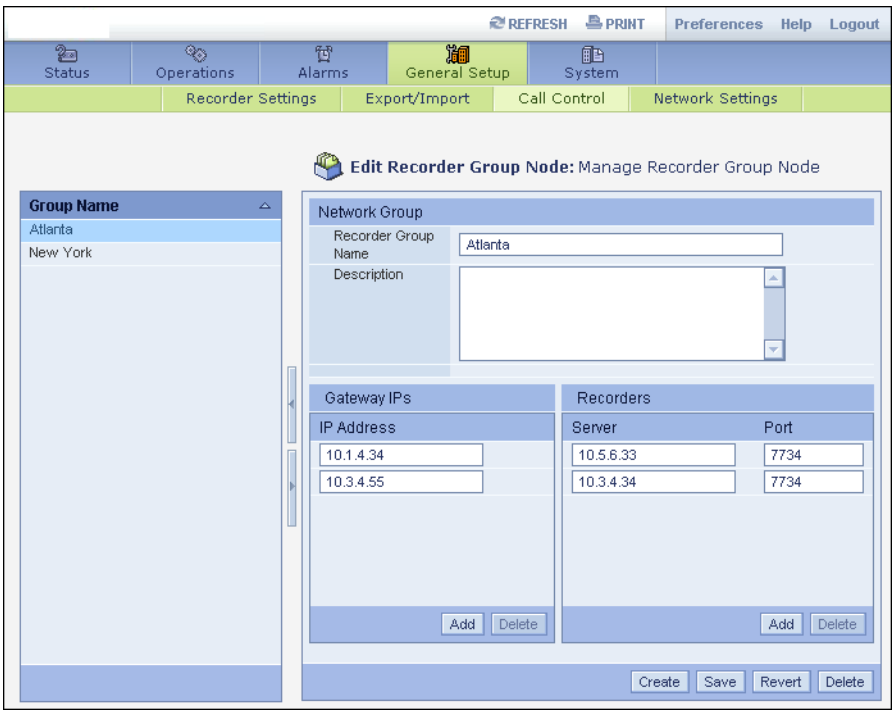
Editing a Call Control Recorder Group

Edit Recorder Group information to change a Recorder group name or description, or to type new call control gateway or Recorder information. All editing is done in real time and there is no Edit button.

To edit a Recorder group

1 Click **General Setup > Call Control** and in the Recorder Group pane on the left, select a Recorder group. Information about the group displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Edit any displayed information or add new gateway or Recorder information as described in Creating a Call Control Recorder Group on page 179.

3 Click **Save**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Chapter 4

Managing System Components

Managing System Components describes how to manage and monitor each of the TDM or IP Recorder system components using the Recorder Manager. This includes using component information for tasks such as licensing, exporting and importing logs and settings. To perform any of these tasks you must be authorized to access all features.

Information is described in the following topics:

- Monitoring Components with Alarms
- Using Component Information

Monitoring Components with Alarms

Monitor Recorder components by using alarms triggered by predefined and programmed events and conditions. Whenever an alarm is triggered, a component is providing information that allows you and other defined e-mail recipients to react to, and resolve, the reported changing of conditions in one or more Recorders.

Alarm information is described in the following topics:

- Configuring Alarms
- Viewing and Monitoring Alarms
- Setting Alarm Notification Profiles
- Configuring E-mail Servers
- Configuring SNMP Nodes

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Alarms

Configure Alarms to set up the presentation of the various alarms raised by a Recorder, such as whether the alarm sounds and who should be notified. These are the same alarms that display in the Enterprise Manager when triggered. Alarms can be resolved either from the Enterprise Manager or from the local Recorder Manager, though configuration can be done only from the Recorder Manager. Information is presented in the following topics:

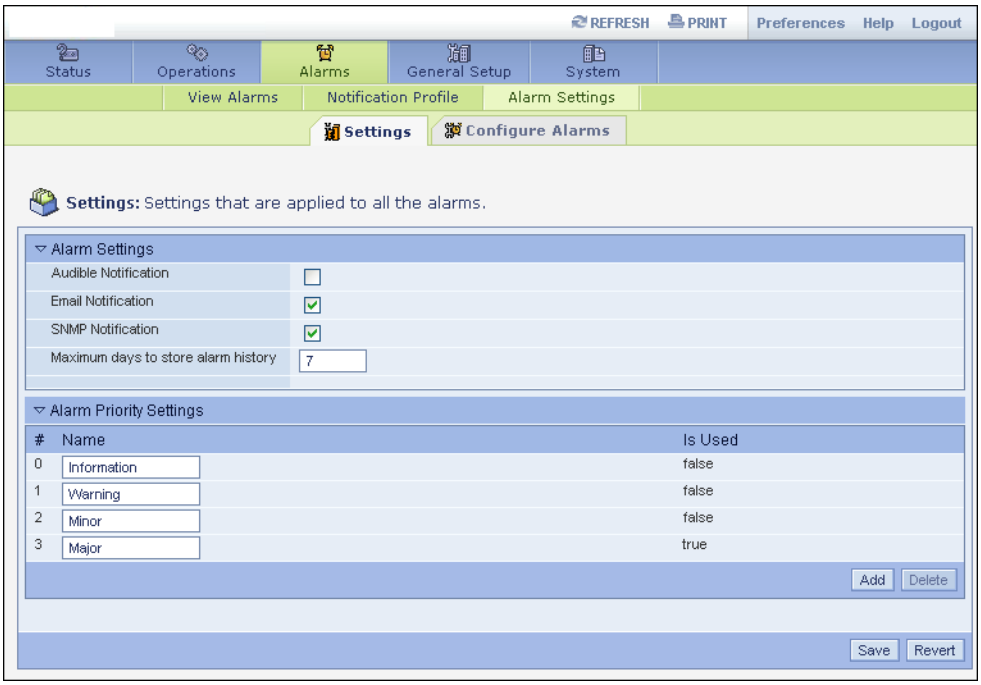
- Viewing Alarm Settings
- Editing an Alarm
- Assigning Schedules and Profiles to Alarms

Viewing Alarm Settings

View alarm settings (configurations) to view global settings for alarms. You can set all alarms to be audible, to be e-mailed to specified recipients, and the number of days alarms are to be retained in history, unless cleared by a user. You can also set priorities for each alarm.

To view alarm settings:

1 Choose **Alarms** > **Alarm Settings** > **Settings**.



© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

2 Complete the fields in the **Alarm Settings** screen as follows:

Field	Description
Alarm Settings	
Audible Notification	Check to indicate if a sound will accompany an alarm. This field is checked by default. If unchecked, you can still apply the setting to the individual alarm, as described in Editing an Alarm on page 187. Audible notifications set on this screen determine whether alarms set at the individual alarm level are enabled or disabled. The Audible Notification you set here is the global setting, which overrides the local setting.
E-Mail Notification	Check to indicate if e-mail notifications will be sent when the alarm is raised. This field is checked by default.
SNMP Notification	Check to specify if the system will use SNMP (Simple Network Messaging Protocol) traps to send alarm notifications.
Max days to store alarm history	Type the maximum number of days that an inactive alarm should be displayed as history. The default for this field is 30 days. After this, the inactive alarm (in alarm history) is deleted.
Alarm Priority Settings	
Priority	Shows the read-only value of the alarm priority, beginning at zero.
Name	Shows the name of the alarm priority. Four default alarm priorities are given: Information, Warning, Minor, and Major, representing severity levels for each alarm. You can customize default alarms at any time by renaming the default fields and values then clicking **Save**. You can also add new alarm priorities as well as delete unassigned alarm priorities. **To add an alarm priority:** 1. Click **Add**. A new alarm priority with a value of 9 (the highest) is added). 2. Enter a name for the new alarm priority. 3. Change the priority value from 9 to the desired value. 4. Click **Save**
Is used	Shows **True** if the alarm priority has been applied to an alarm, and **False** if it has not be applied to an alarm.

3 Do one of the following:

- Click **Add** to append a new alarm priority level to the list, using the next available number. The **Is used** column shows **False** until the priority is assigned to an alarm.
- Click **Delete** to delete an alarm priority, providing it has not been assigned. If a priority is assigned to an alarm, it cannot be deleted until you unassign the alarm.

4 Click **Save**.

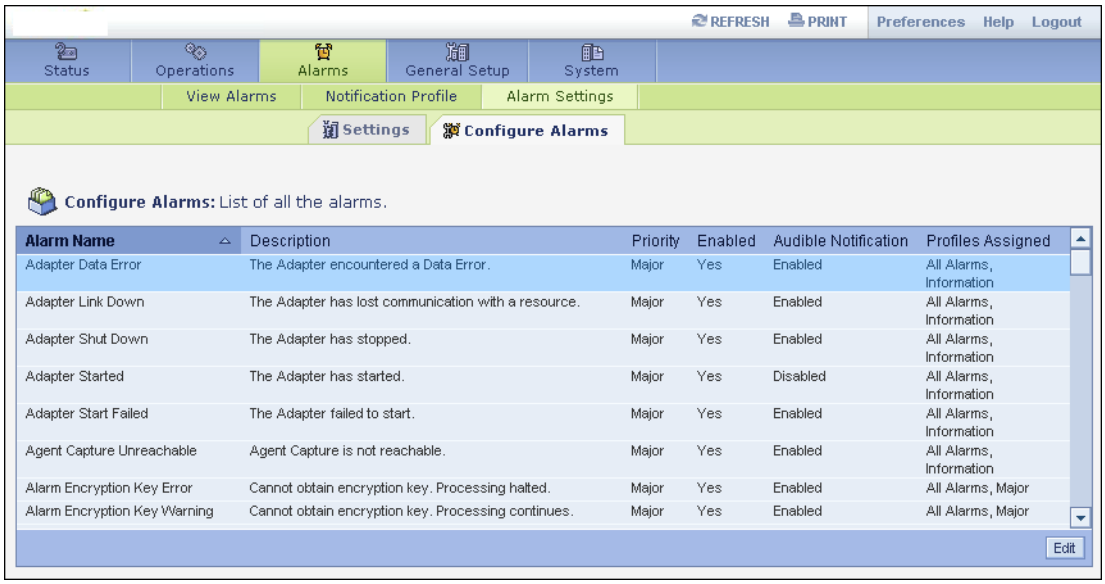
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Editing an Alarm

Edit an alarm from the Configure Alarms window to indicate if it will give off a sound, create an e-mail notification and to specify the number of days an inactive alarm will be stored in history.

To edit an alarm:

1 Choose **Alarms** > **Alarm Settings** > **Configure Alarms**. The Configure Alarms screen displays a summary of all alarms.



2 Review the summary (all fields are read only) of alarm profiles:

Field	Description
Alarm Name	Shows the names of alarms currently assigned to profiles. For a listing of all system alarms, refer to on page 243.
Description	Shows a brief description of the purpose of the alarm.
Enabled	Shows Yes or No to indicate if the alarm is active (enabled) or not active. Global settings, which override local settings, are described in Viewing Alarm Settings on page 185. Local settings, where you edit individual alarms, are described in Assigning Schedules and Profiles to Alarms on page 188.
Priority	Shows the priority level for this alarm, as described in Viewing Alarm Settings on page 185.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Audible Notification	When enabled an audible sound is created on both the Recorder and the Recorder Manager when the alarm is triggered. When disabled no audible sound is heard when the alarm is triggered. Shows as either Enabled or Disabled. As with the Enabled field described above, global settings override local settings.
Profiles Assigned	Profiles of individuals or departments who will be notified by e-mail when the associated alarm is raised. This field is blank if no profile has been assigned.
Counter Alarms	Shows alarms that have business rules where the user sets thresholds settings, so that when a threshold is reached or exceeded, an alarms is raised.

3 Click **Edit** with an alarm profile selected. (If no alarm is selected, the **Edit** button is disabled.) The Alarm Settings window displays.

4 Follow the steps in Assigning Schedules and Profiles to Alarms on page 188.

Assigning Schedules and Profiles to Alarms

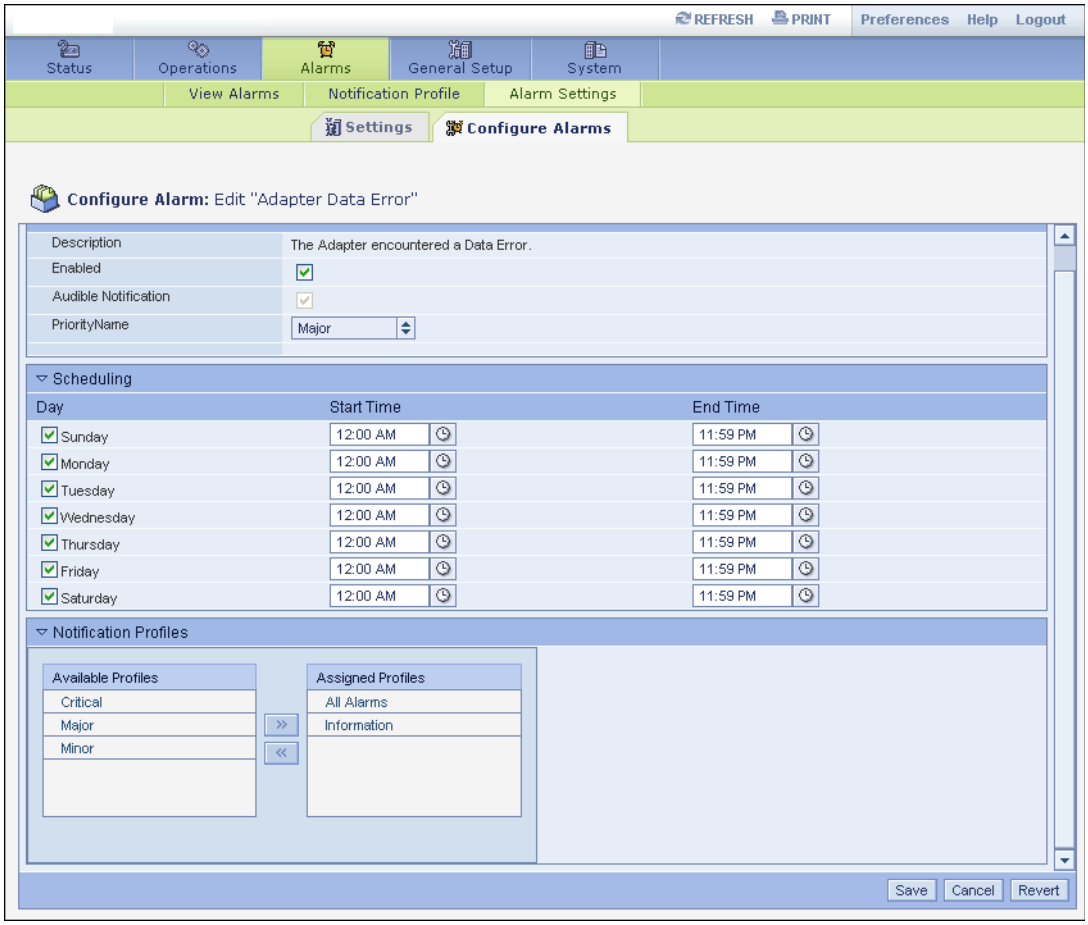
Assign alarm settings, alarm schedules, and alarm notification profiles to a single alarm to provide local alarm settings, times when the alarm is active, and to specify which parties will be notified by email when the alarm is triggered.

To assign profiles to alarms:

1 Click **Alarms** > **Alarm Settings** > **Configure Alarms**. The Configure Alarms screen displays a summary of all alarms as described in Editing an Alarm on page 187.

2 Select an alarm, and then click **Edit**. The Configure Alarm window displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



3 Review and edit fields according to the following:

Item	Description
Description	Shows a brief, read-only description of the alarm. For details of all Recorder alarms, refer to on page 243.
Enabled	Check to enable or disable the alarm. A checkmark indicates that the alarm is enabled (active) and that assigned profiles will be notified by email when the alarm is triggered. If disabled, no alarm notification is made.
Audible Notification	Check to indicate that the alarm is to emit a warning sound when triggered. This is the local setting, which can be overriden by the global setting described in Viewing Active Alarms on page 191.
Priority Name	Select a priority level for this alarm. Default settings are **Information**, **Warning**, **Minor** and **Major**. You can change these names as well as add more alarm priorities, described in Viewing Alarm Settings on page 185.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Item	Description
Scheduling	Allows you to specify Start and End times for each day of the week when the alarm is to be in effect. Click the Clock icon to open the Time window and set times, or enter times in the format hh:mm:AM/PM
Notification Profiles	Allows you to select a profile from the **Available Profiles** window and by clicking the right-pointing arrow move that profile to the **Assigned Profiles** window on the right. Reverse this process to remove alarm notification profiles from this alarm. See Creating or Editing an Alarm Notification Profile on page 197 for more information.

4 Click **Save**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Viewing and Monitoring Alarms

Monitor alarms to view a list of all active alarms and corresponding alarm details and history. You can also view alarm summary information, silence an audible alarm, clear alarm history and see at a glance which alarms need to be resolved.

This information is described in the following topics:

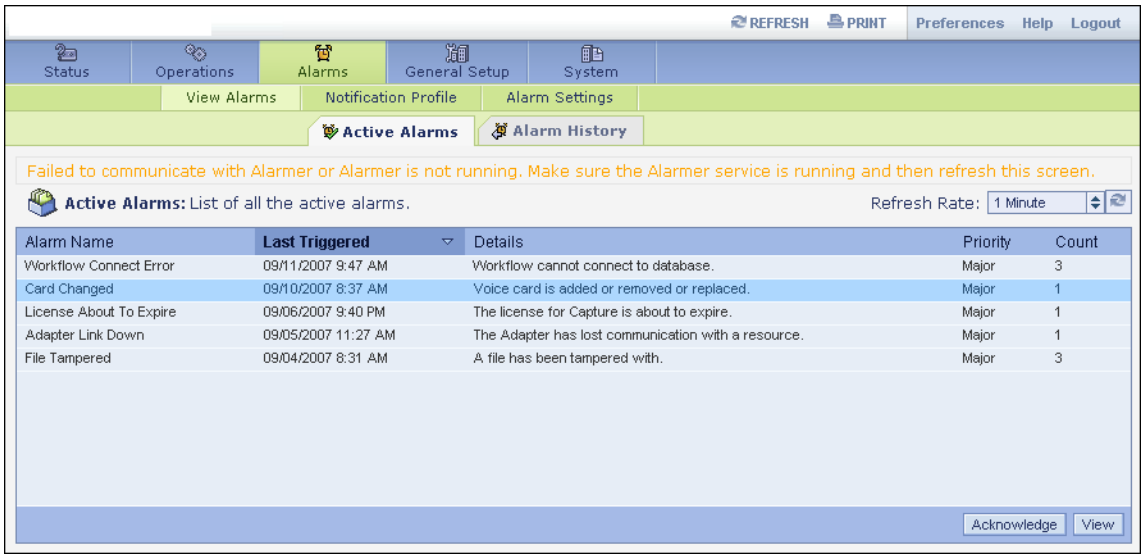
- Viewing Active Alarms
- Acknowledging Alarms
- Clearing Alarm History

Viewing Active Alarms

View active alarms that have been triggered to obtain details of the alarm as a basis for taking corrective action. When you are notified of an alarm, either by email or from an audible notification, or other method, you visit the Active Alarms window to resolve the alarm.

To view and silence an alarm:

1 Choose **Alarms** > **View Alarms** > **Active Alarms**. The Active Alarms screen displays showing a Silence button (not shown) in an Alert message.



2 Click **Silence**. The audible sound is turned off in both the Recorder and in the Recorder Manager.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 Review fields according to the following:

Item	Description
Alarm Name	The short name for the alarm. For a complete list of alarms, refer to on page 243.
Last Triggered	Date when the alarm was last triggered, based on the time zone settings specified in the Recorder Manager. This may provide trend information to assist in troubleshooting.
Details	Shows a full description of the alarm, as in the Alarms Summary above.
Priority	Shows the priority of the alarm, as described in Viewing Alarm Settings on page 185.
Count	The number of instances of the alarm currently triggered.

4 Do one of the following:

- Click **View** to view the full text message of the selected alarm and any resolution suggestions. A complete list of alarm messages appears in Alarms Summary on page 244.
- Click **Acknowledge** to acknowledge that you have seen this alarm, as described in Acknowledging Alarms on page 192. The alarm is then removed from this window and placed in history.
- Set the **Refresh Rate** by clicking the up and down arrows. The time showing as the Refresh Rate represents the frequency of database checks. For example if the refresh rate is set to one minute, the Alarmer component checks the database every minute for new alarms. If the Refresh Rate is set too high, alarms sound on the Recorder but do not display in Recorder Manager until the scheduled Refresh Rate interval. If the Refresh Rate is set too low, system performance may be affected as the Alarmer then checks the database frequently, using up system resources.

Acknowledging Alarms

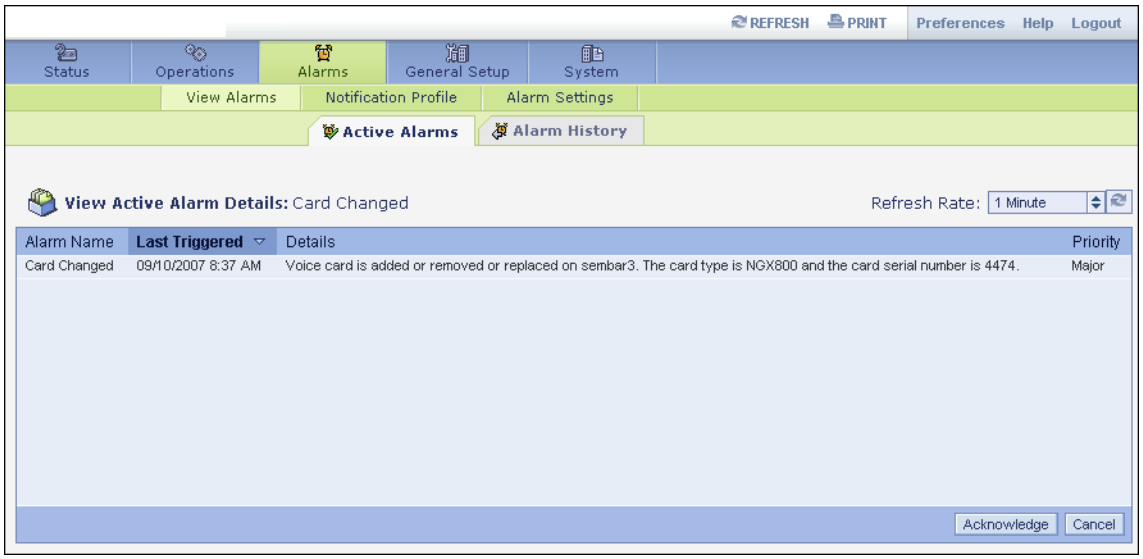
Acknowledge an alarm once you have silenced it to move all instances of the alarm to the Alarm History screen. Certain types of alarms are moved automatically to the history section without human intervention, if the condition gets fixed. For a summary of all system alarms, refer to on page 243.

To acknowledge alarms:

1 Choose **Alarms** > **View Alarms** > **Active Alarms**. A listing of all active alarms displays.

2 Select an Alarm and click **View**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



3 Review each alarm according to the following:

Field	Description
Alarm Name	The name of the alarm. For a complete list of Recorder Alarms, refer to Alarms Summary on page 244.
Last Triggered	Date when the alarm was last triggered, based on the time zone settings specified in the Recorder Manager. This may provide trend information to assist in troubleshooting.
Details	Shows a detailed description of the alarm. For a complete list of Alarms, refer to on page 243.
Priority	Shows the priority of this alarm, as described in Viewing Alarm Settings on page 185.
Refresh rate	See detailed description in Viewing Active Alarms on page 191.

Note: If archive devices are changed, for example a new device added with a new name, then old alarms may need to be cleared manually in the Recorder Manager as they will not be cleared automatically.

4 Take the necessary action to resolve each alarm and then click **Acknowledge.**

5 Click **OK** to confirm that you wish to acknowledge the selected alarms.

The selected alarm type and all its instances are made inactive and moved to Alarm History.

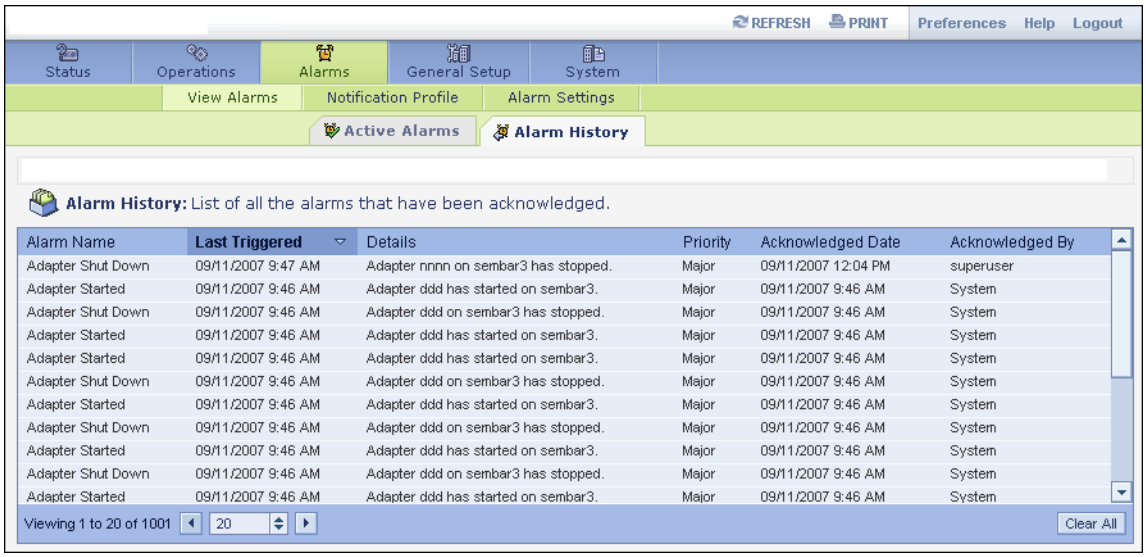
Clearing Alarm History

View alarm history to review a cumulative list of alarm details and remove records that are no longer useful. Some alarms may be resolved by the system, in which case they are listed here as being resolved by a system component.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To clear alarm history:

1 Choose **Alarms** > **View Alarms** > **Alarm History**.



2 Review the Alarm History window, according to the following:

Field	Description
Alarm Name	Shows the name of the alarm. For a complete list of Recorder alarms, refer to on page 243
Last Triggered	Shows the date when the alarm was last triggered, based on the Time Zone settings set in the Recorder Manager. This may provide trend information to assist in troubleshooting.
Details	Shows a detailed description of the alarm and its resolution.
Priority	Shows the priority of the alarm, as described in Viewing Alarm Settings on page 185.
Acknowledged Date	Shows the date and time on which the alarm was acknowledged, based on the Time Zone settings set in the Recorder Manager.
Acknowledged By	Shows the name of the person or department who acknowledged the alarm. For alarms that were resolved by the system, the responsible system component displays.
Pagination	Click to go to another page that allows the viewing of additional alarms in other pages. You can choose a value for the number of alarms to display per page by clicking the up/down arrows to the right of the display area.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 Click **Clear All** to remove all alarm instances from the Alarm History screen. If you do not clear alarms, they are cleared automatically according to **Maximum days to store alarm history** described in Viewing Alarm Settings on page 185

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Setting Alarm Notification Profiles

Set alarm notification profiles associated with specific recorder alarms to add the profile of another system administrator or user who will be notified by email when the alarm is triggered. You can also directly edit and delete a profile from this area of the Recorder Manager. These tasks are described in the following topics:

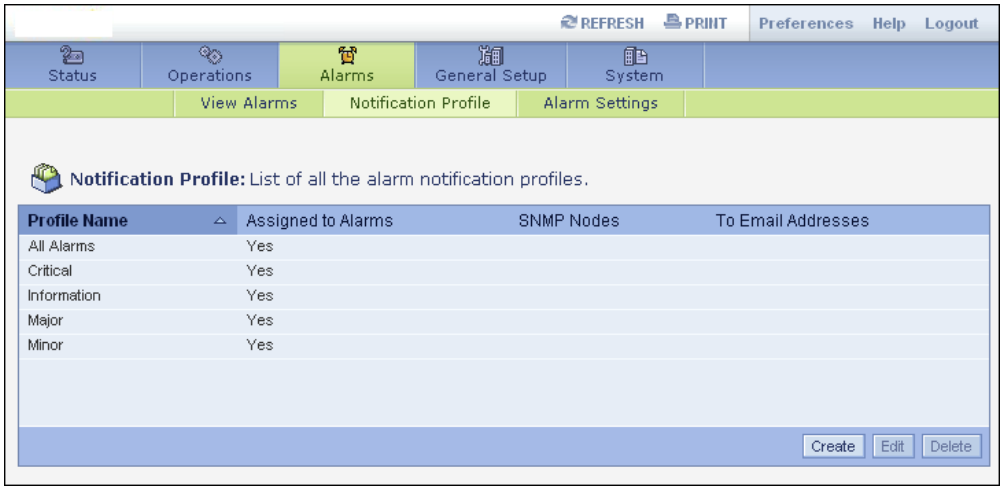
- Reviewing Alarm Notification Profiles
- Creating or Editing an Alarm Notification Profile
- Deleting an Alarm Notification Profile

Reviewing Alarm Notification Profiles

Review alarm notification profiles to assess current profile names and e-mail addresses of the one or more persons who will be notified when an alarm is triggered. From this information you can also determine if profiles must be created, edited, or deleted.

To review alarm notification profiles:

1 Choose **Alarms** > **Notification Profiles**. A list of alarm notification profiles is displayed.



2 Select a Notification Profile according to the following:

Field	Description
Profile Name	Shows the name assigned to the Alarm notification
SNMP Nodes	Shows the name of the SNMP nodes (Simple Network Management Protocol) as created in SNMP configuration.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Assigned to Alarm	Shows a Yes/No list indicating if the alarm (as more than one alarm can be assigned to a profile) has been assigned to the selected notification profile.
E-Mail Addresses	Shows the e-mail addresses of alarm notification profiles assigned to the alarm, separated by a comma or semicolon. There can be zero or many addresses listed here.

3 Click **Create, Edit,** or **Delete** to add a new profile, edit an existing, selected, profile, or delete a profile, respectively**,** as described in Creating or Editing an Alarm Notification Profile on page 197 and Deleting an Alarm Notification Profile on page 199.

Creating or Editing an Alarm Notification Profile

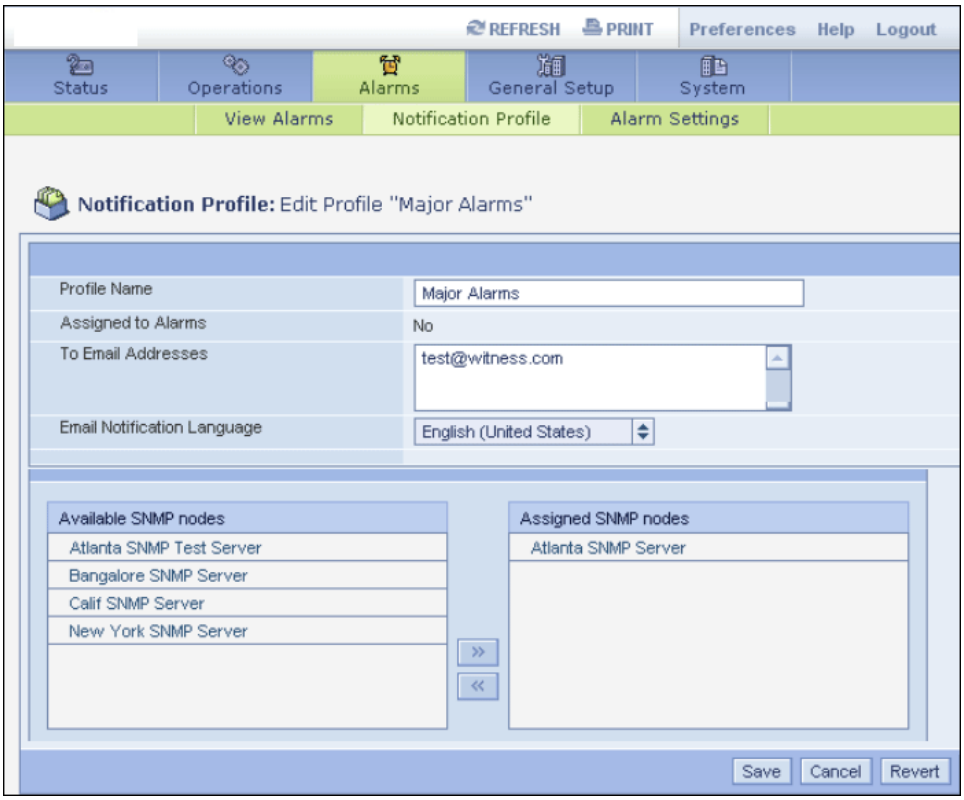
Create a new alarm notification profile or edit an existing profile to add or edit a recipient to be notified by e-mail that an alarm has been triggered. To create a profile click Create. To edit a profile, select a profile and click Edit.

To create or edit an alarm notification profile:

1 Choose **Alarms** > **Notification Profiles**. A list of alarm notification profiles is displayed.

2 Click **Create** or select a profile and click **Edit**. The Alarm Notification Profile screen shows.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



3 Complete or review the fields according to the following:

Field	Description
Profile Name	The name of the profile assigned to the Alarm notification
Assigned to Alarms	Read-only field that indicates if the Profile Name has been assigned to any alarms.
To Email Addresses	The e-mail addresses of alarm notification profiles assigned to the alarm, separated by a comma or semicolon. **NOTE**: There can be zero or many addresses listed here.
Email Notification Language	Dropdown box that allows you to choose the preferred language in which the notification will be made.
Available SNMP nodes	Shows a list of all available SNMP servers/nodes configured in the SNMP configuration. The notification profile must be assigned to a listed node. To assign an available SNMP node, select it and click the right-pointing arrow.
Assigned SNMP nodes	Shows the SNMP node(s) that has/have been assigned to the current notification profile. To remove an Assigned SNMP node, select it and click the left-pointing arrow.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

4 Click **Save**.

Deleting an Alarm Notification Profile

To delete an alarm notification profile:

1 In the **Alarm Notification** window, select an alarm notification profile.
2 Click **Delete**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring E-mail Servers

Configure e-mail servers to identify the server and to add and test e-mail settings that will be used for notifying specified e-mail recipients about component or event alarms. E-mail server settings include a host IP address, port number, and an option to include a username and password if needed. In this way, email notifications can be made automatically. This information is presented in the following topics:

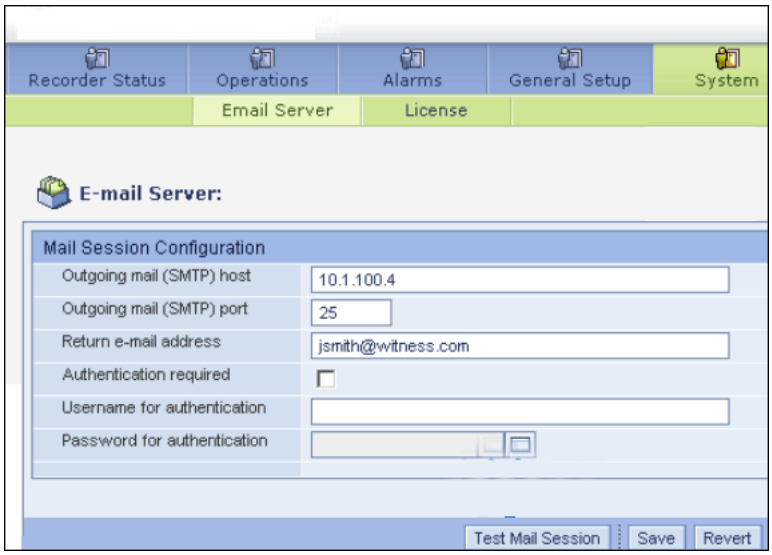
- Configuring E-mail Server Settings
- Testing Email Settings

Configuring E-mail Server Settings

Add e-mail server settings to set up outgoing mail and specify authentication particulars. This enables specified e-mail recipients to be notified automatically when a component or event alarm is triggered.

To configure e-mail server settings:

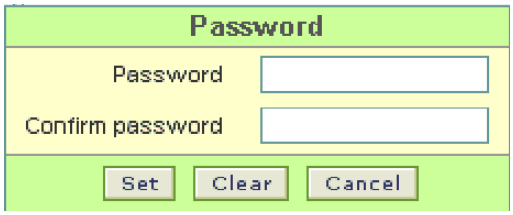
1 Click **System** > **E-mail Server**. The Mail Session Configuration screen displays.



2 Complete the Mail Session Configuration fields as follows:

Field	Description	Entry Required?
Outgoing mail (SMTP) host	The host name or IP address of the outgoing mail host.	Required
Outgoing mail (SMTP) Port	The 5-digit outgoing mail port number. Default is 25.	Required

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description	Entry Required?
Return e-mail address	The source (From) e-mail address used for the test of e-mail server settings.	Required
Authentication required	Checkbox indicating that a specified user name must be used to authenticate the e-mail. If this is checked, the Username and Password fields must be completed.	Optional
Username for authentication	The Username to be used to authenticate the e-mail if the E-mail Authentication checkbox is checked.	Required (if **Authentication required** is checked)
Password for authentication	Used to type a password to be used along with the Username in the previous field if the E-mail Authentication checkbox is checked. Clicking the folder icon opens the Password dialog box.  Type the password, confirm the password, and click Set.	Required (if **Authentication required** is checked)

3 Click **Save**.

Testing Email Settings

Send a test e-mail to ensure that the specified e-mail server settings work properly. In this way, the specified e-mail recipients are assured of being notified that one or more component alarm has been triggered.

To test e-mail settings:

1 Complete the fields in the e-mail server settings window as described in Configuring E-mail Server Settings on page 200.

2 Click **Test Mail Session.**

- If settings are correct, a test e-mail is sent to the **Return e-mail address** specified in the e-mail server settings.
- If the test e-mail does not arrive, re-type the SMTP settings and make sure the return e-mail address is valid. If settings appear OK and the test still does not work, uncheck **Authentication required** and try again.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring SNMP Nodes

Configure SNMP nodes to manage the SNMP (Simple Network Messaging Protocol) node information used for alarm notifications. SNMP trap configurations, once created, are used in setting up alarm notification profiles, where one or more of the SNMP trap configurations is selected.

If the Network Management System (NMS) you are using requires loading the MIB to view the trap messages, please load the Management Information Base (MIB) files from the Recorder Installation DVD at the following location: **`RecorderInstallation\WITS MIB`.** Please contact your network administrator for assistance in how to load MIBs in the NMS.

Information is presented in the following topics:

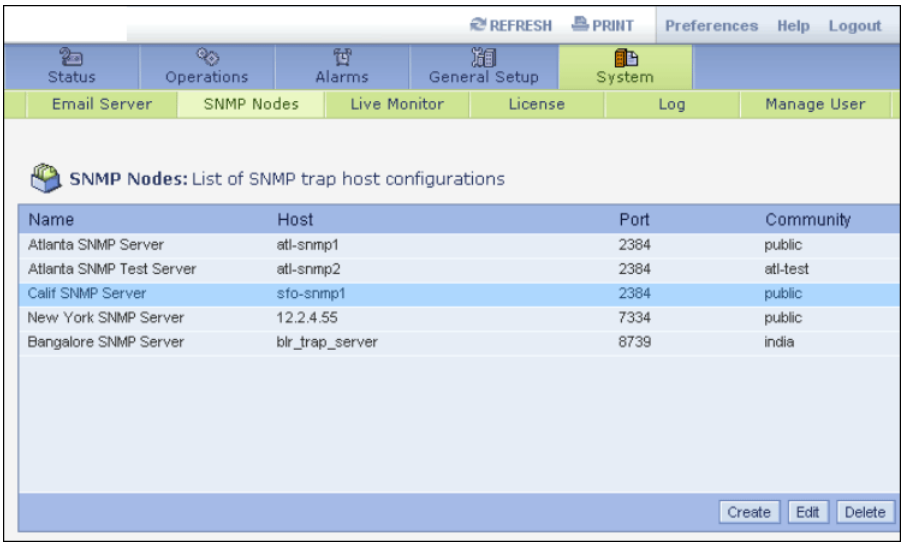
- Viewing SNMP Nodes
- Creating and Editing SNMP Nodes
- Deleting SNMP Nodes
- Configuring HP SIM for SNMP – an example.

Viewing SNMP Nodes

View SNMP nodes to review information associated with SNMP nodes within the organization. These nodes support alarm notification: alarm messages are created from SNMP traps and use SNMP server settings for communication within the network.

To view SNMP servers:

1 Choose **System** > **SNMP Nodes**.



© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

2 Review the SNMP Node screen according to the following:

Field (all required)	Description
Name	The name of the SNMP trap configuration, such as Atlanta SNMP Server.
Host	The name or IP address of the server the SNMP trap message will be sent to.
Port	The port on the PC to which the SNMP traps are sent, such as 162.
Community	The name used to identify the group to which SNMP devices and management stations belong. The *community* name acts as a weak password when sending the trap message, especially to network management systems (NMSs) that ignore traps that don't have an appropriate community string.

3 Click **Create** or **Edit** to create or edit new SNMP servers, as described in Creating and Editing SNMP Nodes on page 203.

Creating and Editing SNMP Nodes

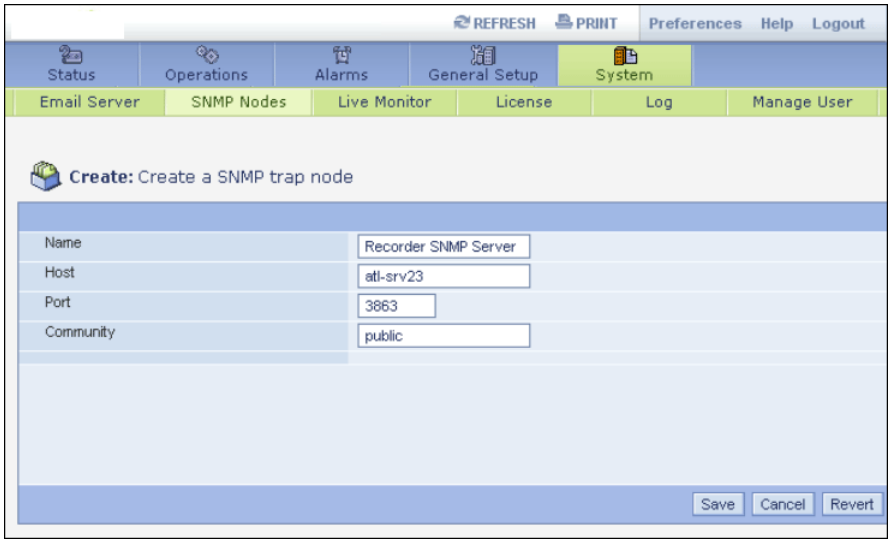
Create and edit SNMP nodes to facilitate alarm notifications to specified notification profiles by using the same window to set up a new SNMP node or edit an existing one.

To create and edit SNMP nodes:

1 Complete the steps described in Viewing SNMP Nodes on page 202 and do one of the following:

- To create a new SNMP node, click **Create**.
- To edit a displayed SNMP node, select it and click **Edit**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Complete the SNMP server screen fields as described in Viewing SNMP Nodes on page 202.

3 Click **Save**.

Deleting SNMP Nodes

Delete SNMP nodes to remove the SNMP trap configuration and all associated notification profiles from the Recorder.

To delete SNMP nodes:

1 Choose **System** > **SNMP Nodes**. The SNMP Nodes screen displays a list of SNMP servers.

2 Select one or more entries and click **Delete**.

If a SNMP trap configuration is deleted, all the notification profiles are updated to remove the reference to the deleted item.

Configuring HP SIM for SNMP – an example

Follow this procedure to import MIBs into an HP SIM server, such as HP Openview, to support SNMP trapping.

1 Collect the MIBs needed for the HP SIM, namely:

- WITS-PRODUCTS-MIB.mib
- WITS-CSFAMILY-MIB.mib
- WITS-CS-MIB.mib
- WITS-TRAP-MIB.mib

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

2 Copy these files to the MIBs directory on the HP SIM server. They must be in this location or the compile does not work, unless you make changes to the command line.

3 Compile the MIBs in the correct order using the **mcompile** command from a DOS prompt in the same order as above. Once compiled the MIBS are converted to configuration files (CFG's). However, these CFGs do not work until you complete the next step.

4 Edit the compiled MIBS (now CFG's) as follows:

- For WITS-PRODUCTS-MIB.cfg, make sure the following lines are in the file:

—witsRegMIB OBJECT IDENTIFIER ::= { enterprises 1815 }

—witsProducts OBJECT IDENTIFIER ::= { witsRegMIB 1 }

- For WITS-CSFAMILY-MIB.cfg, make sure the following lines are in the file:

—witsRegMIB OBJECT IDENTIFIER ::= { enterprises 1815 }

—witsProducts OBJECT IDENTIFIER ::= { witsRegMIB 1 }

—witsCSFamily OBJECT IDENTIFIER ::= { witsProducts 1 }

- For WITS-CS-MIB.cfg, make sure the following lines are in the file:

—witsRegMIB OBJECT IDENTIFIER ::= { enterprises 1815 }

—witsProducts OBJECT IDENTIFIER ::= { witsRegMIB 1 }

—witsCSFamily OBJECT IDENTIFIER ::= { witsProducts 1 }

—witsCS OBJECT IDENTIFIER ::= { witsCSFamily 1 }

- For WITS-TRAP-MIB.cfg, make sure the following lines are in the file:

—witsRegMIB OBJECT IDENTIFIER ::= { enterprises 1815 }

—witsProducts OBJECT IDENTIFIER ::= { witsRegMIB 1 }

—witsCSFamily OBJECT IDENTIFIER ::= { witsProducts 1 }

—witsTraps OBJECT IDENTIFIER ::= { witsCSFamily 2 }

—trapGroups OBJECT IDENTIFIER ::= { witsTraps 99 }

5 Register the CFG's in the HP SIM using the following command:

Mxmib -a <Compiled MIB file**>.** For example, **Mxmib -a WITS-PRODUCTS-MIB.CFG**

6 Configure HP SIM to change the Alerting level on the MIB to whatever status is appropriate. The status of Critical is recommended.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Using Component Information

Use component configurations and logs to diagnose problems, exchange configurations, and serve as backups. You can export and import component configurations as well as export and clear component logs. Recorder licensing is also included as component information, as this provides details of the number of licensed channels and other details. These tasks are described in the following topics:

- Exporting and Importing Configuration Information
- Exporting and Clearing Component Logs

Exporting and Importing Configuration Information

Export and import configuration information to save and restore a copy of the Recorder's configuration files (for emergency backup purposes). If for some reason the configuration file is deleted or corrupted you can restore an imported configuration file(s). Configuration files differ by Recorder type. However you never need to specify file names as they are provided by Recorder Manager. To export or import configuration information, simply click the Export or Import button. The file name with the current time stamp added displays.

The Recorder stops recording to allow the import. Similarly, you can export the configuration file to another Recorder. This is accomplished by exporting and importing configuration information using the Recorder Manager. Different information displays, depending on the server type (Voice or Screen Recorder, or IP Analyzer).

This information is described in the following topics:

- Exporting Configuration Information
- Importing and Restoring the Configuration File

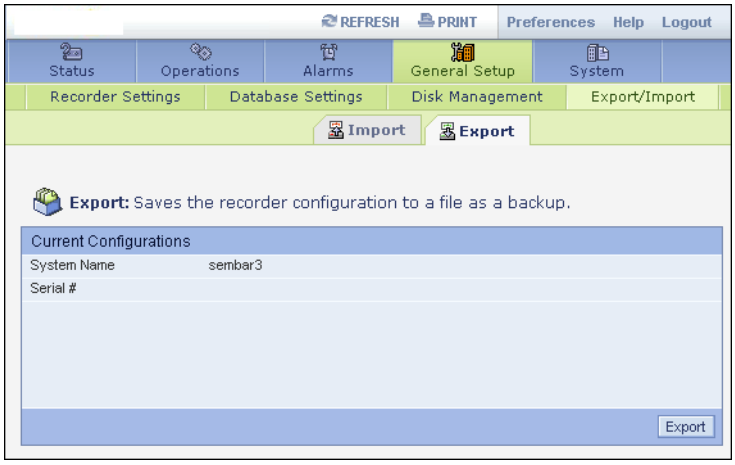
Exporting Configuration Information

Export configuration information to save a copy of the main Recorder configuration file to a secure disk location for backup purposes. This file contains configuration information on the capture engine, consolidator, disk manager, local archive, workflow, alarms, and other Recorder components.

To export configuration information:

1 Choose **General Setup > Export/Import > Export.** A summary of the Recorder's configuration displays.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 Click **Export**. The File Download window displays

3 In the file download window, click **Save** to save the Recorder's configuration file. (See Exporting and Importing Configuration Information on page 206 for more information).

4 Complete the export window by specifying a target location for the exported configuration file.

It is recommended that the target location be a secure location on a different drive that can be easily accessed in case the file needs to be used to restore a corrupted or deleted configuration file.

The file exported contains the date in the file name.

Importing and Restoring the Configuration File

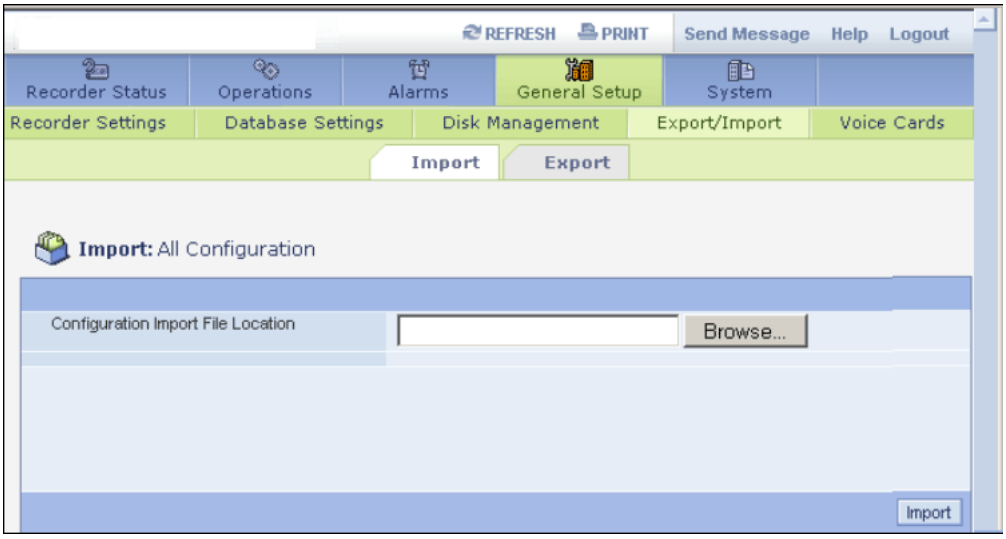
Import the configuration file to restore a copy of the main Recorder configuration file. Configuration files contain information on the capture engine, consolidator, disk manager, local archive, workflow, and alarms, and, live monitor state (if installed) components, so that once the file(s) is imported, all configuration information is restored.

The Recorder stops recording when a configuration file is imported. A warning displays in Recorder Manager, warning of potential disastrous effects from importing an incompatible configuration file.

To import and restore the configuration file:

1 Choose **General Setup** > **Export/Import** > **Import.**

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.



2 For Configuration import File Location, type the path where the configuration file is located (see Exporting and Importing Configuration Information on page 206 for more information) or click **Browse** and locate this file.

3 Click **Import**. A summary of configuration information displays, including Recorder name, serial number, and the date the file was exported.

4 Click **Save** when prompted to accept the import. The existing configuration file is replaced with the imported one.

5 Restart the Recorder as described in Starting and Stopping the Recorder and Components on page 59.

Exporting and Clearing Component Logs

Export component log files to another location to allow for the sharing and comparison of component information between Recorders. You can also manually clear a component's logs to free disk space or remove conflicting logs. Components for which log files are created include Alarms, Archiver, Calls Consolidator, Capture, Compressor, Disk Manager, Live Monitor State, Maintainer, Retriever, and Web Services. Different components display according to the installation type (Voice or Screen Recorder, or Analyzer).

Information is described in the following topics:

- Exporting Component Logs
- Clearing Component Logs

Exporting Component Logs

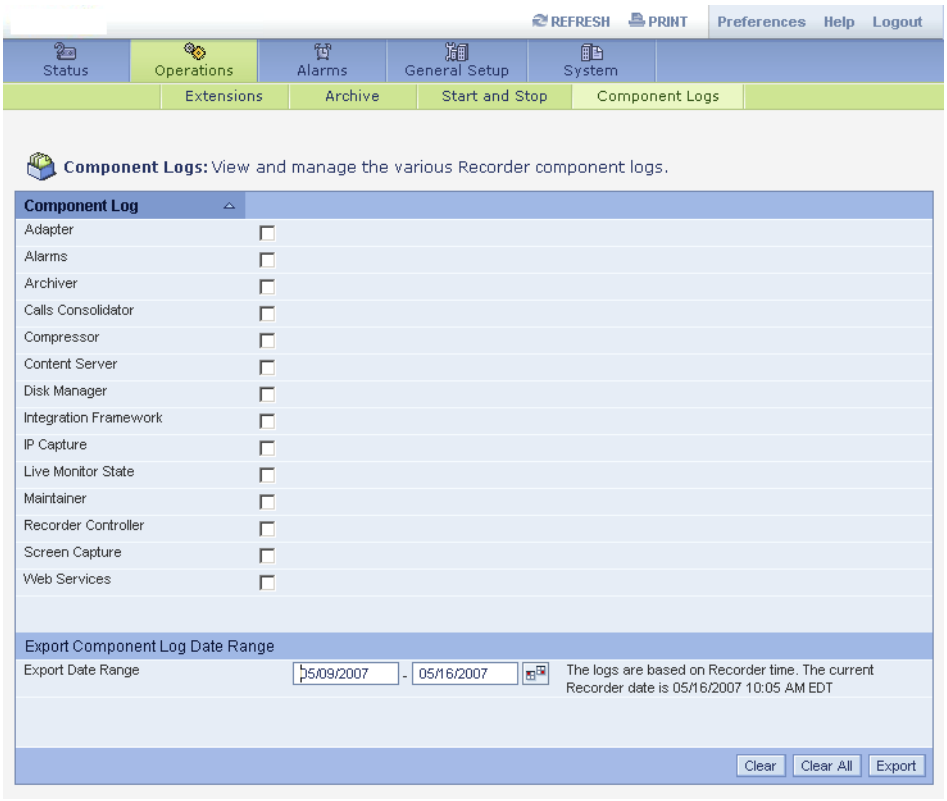
Export component logs to export a copy of one or more of the Recorder's available component logs. Logs available for export include logs that show audit trails for

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Recorder components. You can use component logs for information sharing as well as for troubleshooting.

To export component logs:

1 Choose **Operations > Component Logs**. The Component Logs screen display.



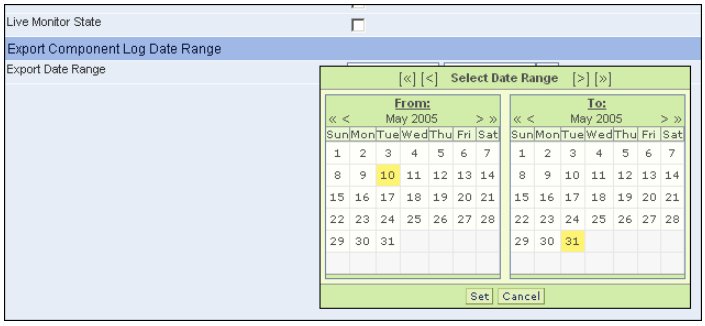
2 Under **Component Log** choose one or more components to have logs exported according to the following:

Item	Description
Adapter	Logs from the CTI adapter showing activity only if Integration Service is present
Alarms	Logs from the alarmer component showing alarm activity from this Recorder.
Archiver	Logs from the archiver component showing archive activity from this Recorder.
Call Consolidator	Logs from the consolidator component showing media database activity.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Capture (can be TDM, or IP)	Logs about calls recorded from the TDM or IP capture engine, depending on your installation type for this Recorder. That is, in a TMD Recorder (ITS IP Recorder), TDM Capture shows, and in an IP Recorder, IP Capture shows.
Compressor	Logs about compressor activity in compressing IP calls or uncompressed TDM calls from Cybertech cards on this Recorder.
Content Server	Logs from the Content Server component, which stages contacts being retrieved by Search and Replay.
Disk Manager	Logs from the disk manager component, showing call buffer activity on this Recorder.
Integration Framework	Logs from the Integration Framework, showing activity only if IS is used on this Recorder.
Live Monitor State	Logs from the live monitor state component showing live monitor activity from this Recorder.
Maintainer	Logs from the maintainer component, which controls files to and from the Workflow component.
Recorder Controller	Logs about the Recorder Controller type being used (can be CTI Controlled, Unify Controlled, or Recorder Controlled).
Screen Capture	Logs about screen recordings from the screen capture engine.
Web Services	Logs from the Recorder's web services component which coordinates the flow of information to external services such as SNMP services and licensing.

3 Under **Component Log Date Range**, define an export date range by clicking the icon to the right of the date range field. The Export Date Range window displays.



4 In the **Select Date Range** window, define the date range as follows: in the left (From) pane, click a start date, and in the right (To) pane, click an end date and then click **Set**. The selected dates are inserted into the **Export Date Range** fields.

5 Click **Export**. The File Download window displays.

6 Click **Save** and save the file to a location on the hard disk or to a network location.

You may receive a timeout warning. Selecting a large range as well as a large number of components to export can take several minutes to generate the zip file of

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

the selected component logs. You will receive a warning message if the file cannot be created within the default time (1 minute). You are then prompted to continue waiting or cancel the operation. Results from cancelled operations are deleted automatically.

Clearing Component Logs

Clear component log files for one or all component(s) to clear (that is, delete) these files and make space for new ones.

To clear component logs:

1 Choose **Operations > Component Logs**.

2 In the Component Logs window do one of the following:

- Select one or more components then click **Clear** to clear log files for all selected components.
- Click **Clear All** to delete the log files of all components. All logs except the current log are deleted when Clear All is selected.

3 Click **OK**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Chapter 5

Performing System Maintenance

System Maintenance refers to daily or regular system operations that you need to do to maintain and troubleshoot the Recorder so that it always runs at an optimum performance level. This includes hardware and software maintenance and hardware and software troubleshooting tasks.

These tasks are described in the following topics:

- Performing Routine Maintenance
- Troubleshooting

Performing Routine Maintenance

Perform system maintenance to ensure that all hardware and software components are operating at peak efficiency. These are tasks that you perform on a regular basis, normally weekly, to obtain maximum flexibility with the Recorder with a minimum amount of service disruption. Performing Maintenance is described in terms of hardware and software and are described in the following topics:

- Performing Hardware Maintenance
- Performing Software Maintenance

Performing Hardware Maintenance

Perform hardware maintenance to ensure that all hardware devices such as media devices and hard drives are working properly and that you can efficiently maintain any component, including replacing that component, at any time. This includes adding an archive device, changing voice cards, changing a hard drive, changing wiring and adding telephone extensions.

This information is described in the following topics:

- Adding or Upgrading an Archive Device
- Changing Voice Cards/NICs
- Replacing a Hard Drive
- Managing Archive Devices
- Rebooting and Restarting

Adding or Upgrading an Archive Device

Add or upgrade an archive drive to archive contacts to an additional location. Existing archive devices may be replaced to upgrade capacity or eliminate a hardware failure. Some USB-based drives may not require a PC shutdown.

To add an archive device:

1. Shut down the PC
2. Connect the drive (DVD, REV drive, or Tape drive) according to the manufacturer's specifications.
3. Restart the PC. Upon restart, the Archiver component detects the added drive and triggers an alarm accordingly.
4. Login to the Recorder Manager and choose **Operations > Archive** to add or edit a drive configuration..

Tape drive takes precedence over the DVD drive in the auto-detect process.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

5 Configure the drive by assigning a drive name, whether it is writable, and whether it is to be auto-ejected, as described in Configuring an Archive Drive on page 67.

6 Click **Save**. The configuration takes effect immediately.

To add an archive media device manually, refer to Replacing a Physical Archive Device on page 74.

Changing Voice Cards/NICs

The Voice Card(s) Auto-Detection feature of the Recorder automatically detects any changes to the hardware configuration on the start-up of the capture component. If any voice cards or NICs have been added or existing ones replaced they are detected automatically and show in the Recorder Manager with one of the following statuses:

Card Status	Description
Newly Added	The card did not exist previously.
Removed	The card has been removed from that slot.
Existing	The card has existed in the system before.
Replaced	Previously existing card of the same type has been replaced with a new card of same type.

To replace a voice card:

1 Stop all the Recorder components as described in Starting and Stopping the Recorder and Components on page 59.

2 Shut down the Recorder host and switch off the power supply.

3 Insert new card(s) or replace existing cards from the Recorder host.

An anti-static cuff is recommended to avoid shocks resulting from static electricity.

4 Restart the Recorder components as described in Starting and Stopping the Recorder and Components on page 59. The capture engine on start-up will automatically detect the hardware changes and raises the appropriate alarm(s).

5 Log in to Recorder Manager and click **Alarms** to view all alarms for voice cards that have been added or removed.

6 Click **General Setup > Voice Cards**. The pane on the left displays the slot number and bus number for all the cards that have been recognized by the Recorder as described in Checking Voice Cards on page 233.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

7 Choose any of the card(s) displayed in the left panel and configure it as necessary and then click **Save**.

Voice cards with a status of **Removed** can be copied but cannot be configured and saved.

8 Restart the Capture Component as described in Starting and Stopping the Recorder and Components on page 59 for the configuration changes to take effect.

Replacing a Hard Drive

Replace a hard drive to increase the capacity of the calls buffer or database storage or to correct a defective hard drive or improve the disk capacity of an existing hard drive. Different procedures exist for the different roles for hard drives. In all cases, you need to initialize, partition, and format the new hard drive. These tasks can usually be completed by using Wizards in the Windows operating system. You can also use DOS commands.

Remember that hard drives must be handled carefully. Avoid static electricity and any magnetic devices such as screwdrivers with magnetic tips. It is strongly recommended that you use an anti-static cuff when handling electronic devices and appliances.

To increase the capacity of the call buffer (Calls Buffer):

1 Back up the Calls as described in To backup the Recorder: on page 226.
2 Shutdown the Recorder components as described in To restart the Recorder's components (Services): on page 219.
3 Shut down the host and replace the hard drive.
4 Restart the host and restore the Calls from the backup on to the new drive.
5 Restart the Recorder components.
6 Log in to the Recorder Manager and choose **General Setup > Disk Management > Drives**.
7 Configure the new drive to be monitored.
8 Restart the Disk Manager component.

To increase the capacity of the databases:

1 Back up the Databases a as described in To backup the Recorder: on page 226.
2 Shutdown the Recorder components as described in To restart the Recorder's components (Services): on page 219.
3 Shut down the host and replace the hard drive.
4 Restart the host and restore the Databases from the backup on to the new drive
5 Restart the Recorder components.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To replace a hard drive containing data only:

1. Back up all the data on the hard drive being replaced to another source such as a backup service or storage area network.
2. Disconnect the old hard drive and reconnect the new hard drive.

For an IDE or SATA hard drive, there are two connector wires: the power connector and the motherboard connector. Sometimes the connection is to a drive controller instead of the motherboard.

3. In Windows Explorer, right-click My Computer and choose **Manage > Storage > Disk Management**. The hard drive you just added appears in the window.
4. If necessary, click **Rescan Disks** to see the new hard drive. If it still does not appear, reboot and try again. If it still does not appear, you may need to press an On/Off/Auto switch in the BIOS. To get to the system BIOS, press F2 or F10, depending on your system, while the machine is booting.
5. When you can see the new disk in Disk Management, right-click and choose **Partition**.
6. Follow screen instructions to **Format** the disk and give the disk a new drive letter.
7. Copy all data from the backup storage device to the new hard drive.

To replace a hard drive containing an operating system and applications:

It is highly recommended that for hard drives containing operating systems and applications you reinstall the operating system and applications to ensure that the registry accurately reflects configurations.

1. Complete all the steps for replacing a hard drive containing data only, until you reach step 7.
2. At step 7, reinstall your operating system and applications.

To swap out a SCSI hard drive:

Swap out a hard drive in a RAID setup by removing the old hard drive and inserting and formatting the new one.

1. Follow procedures described in to replace a hard drive containing data only.
2. At the point where you must format the hard drive, launch your RAID user interface and then format and partition the hard drive.
3. Copy all data from the backup source or allow a mirror disk to copy all information.

Managing Archive Devices

Archiver bundles up individual contacts into files in the TAR format of 100 MB each and copies them on to the media. When the media is full it raises an alarm to indicate that it is full, and prompts the user to replace the media. At the same time, if a label printer is attached it prints a label containing a unique ID number which identifies that specific

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

media and then updates the system database to reflect that those calls are available on that specific media.

You can adapt one of the following back-up and/or media management strategies for your own situation.

- Replace the media on demand. This means that when you are prompted by Archiver that the media is full, you replace the media.
- Replace the media at consistent intervals. Here you replace the media regularly, such as once in a day or twice a day or once in few days depending on the call volume, regardless of whether the media is full or not.
- Conform to requirements. In some organizations, the environment and safety issues dictate how, where, and when the media should be preserved.

To manage archive media:

1. Login to the Recorder Manager and choose **Operations > Archive**.
2. Configure the local Archive as described in Configuring an Archive Drive on page 67.
3. Insert the physical media into the drive.
4. Check the status of the archive media (that is, percent full) by choosing **Recorder Status > Status Summary** in the Recorder Manager.
5. As the media approaches the full threshold, archiver raises an alarm. Once the media is full archiver auto-ejects the media and prints the label.
6. Attach the label to the media and store it offline.

To understand the operation of Archiver:

The following items describes background information needed to perform archive and replay maintenance operations.

Archive

- You can create duplicate copies of media by choosing the Parallel archiving mode as described in Managing Archive Drives on page 66. Then it becomes important to identify duplicate copies with the same label information.
- If a new media is not inserted when the old media is full, Archiver temporarily suspends the archive operations and the contacts are left in the Recorder's call buffer until deleted by the Disk Manager component. It is therefore important to allocate the appropriate amount of disk space for the calls buffer. Refer to Configuring Recorder Settings (Call Buffer) on page 62.
- When contacts are archived, the Archiver component does not delete calls from the call buffer as they 'roll-off' (i.e., are deleted from) the call buffer normally. This is the task of the Disk Manager, as described in Creating Disk Manager Settings on page 77.
- If Archiver encounters any write errors while archiving the calls it suspends the archive

Replay

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- When contacts are retrieved in Search and Replay, if the contact is not available online, Search and Replay prompts for the appropriate, read-only media to be inserted. The media label is the identifier. Then you must locate and insert the appropriate media into the drive.
- Archiver retrieves the requested contact(s) from the media and passes on the Search and Replay to be replayed.
- Retrieved calls are not sorted or re-consolidated.

Rebooting and Restarting

Reboot and restart the Recorder to enforce various degrees of Recorder component start ups. For example, sometimes you will be required to restart the PC to ensure that all components are returned to their original configuration. Other times, you may need to restart only the component in question without rebooting the complete PC. System messages display to advise when a reboot or a restart is required.

To reboot the computer:

Use Recorder Manager to reboot the PC to ensure that the reboot process is conducted in an orderly manner so that no data or configuration information is lost.

1 In the Recorder Manager choose Operations > Start and Stop.

2 Click **Reboot.**

To restart the Recorder's components (Services):

You may need to restart Recorder Services for some routine maintenance tasks such as adding or replacing voice cards, upgrading hardware, or to allow the Recorder's configuration to take effect after it is modified. Normally system messages advise when a restart of components is required.

1 Login to the Recorder Manager and choose **Status > Status Summary**.

2 Check to see if they are any calls currently being recorded.

If there are any calls in progress, stopping the Recorder service(s) results in loss of the calls currently being recorded.

3 Click **Operations > Start and Stop** and stop the Recorder components in the following order:

- Recorder Alarm Service (to prevent unnecessary alarms being raised)
- Recorder Archiver Service
- Recorder Calls Consolidator
- Recorder DiskManager Service
- Recorder LiveMonitor Service
- Recorder Capture (TDM or IP) Service
- Recorder WorkFlow Persistence.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Analyzer Service can be stopped from the Analyzer Manager.

4 Perform the necessary maintenance operation and restart the Recorder by restarting the above services in the reverse order.

5 Log in to the Recorder Manager and click **Alarms** to see if any of the Recorder components have not restarted.

6 Review the Recorder's status by clicking **Recorder Status > Status Summary** as described in Starting and Stopping the Recorder and Components on page 59.

For more information refer to Starting and Stopping the Recorder and Components on page 59.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Performing Software Maintenance

Perform software maintenance to ensure that all software components are working properly and that you can efficiently react to any software issues that may arise, including tasks such as installing a service pack, maintaining Unify scripts, backing up and restoring, defragmenting hard drives, and other software-critical activities. Information is described in the following topics:

- Installing a Service Pack
- Upgrading the Unify Script
- Performing Disk Management
- Changing the Location of the Call Buffer
- Changing a Serial Number
- Managing Agents
- Adding Extensions
- Pruning Contacts
- Backing up and Restoring Contacts
- Duplicating (Cloning) and Combining Recorders
- Swapping the System Database
- Performing Oracle Database Maintenance
- Configuring Oracle Memory (BPMAINDB only)
- Workflow Postgres Database Maintenance

For information on Anti-virus software, refer to the *Recorder Installation Guide*.

Installing a Service Pack

Install service packs from time to time to resolve known bugs or issue and to enhance certain functionality by inserting a supplied CD or DVD and following installation instructions on the screen.

To install a service pack:

1. Review the Software Release Document that accompanies the service pack.
2. If necessary, back up the Recorder as described in Backing up and Restoring Contacts on page 226.
3. Stop the Recorder components as described in Starting and Stopping the Recorder and Components on page 59.
4. Install the service pack as per the instructions in the software release document.
5. Restart the Recorder components as described in Starting and Stopping the Recorder and Components on page 59.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Upgrading the Unify Script

Upgrade the Unify script to if the Recorder is operating in a CTI controlled environment and requires new functionality. Do this by updating the Unify script file and xml file.

Editing the Unify script and XML files is normally performed by developers and is beyond the scope of this document.

To upgrade the unify script:

1. Shutdown the Recorder as described in Rebooting and Restarting on page 219.
2. Back up the existing **`unify.spt`** and **`unify.xml`** files. These are located in the Unify subfolder in your installation directory.
3. Copy the supplied new files **`unify.spt`** and **`unify.xml`** files.
4. Restart the Recorder as described in To restart the Recorder's components (Services): on page 219.

Performing Disk Management

Perform disk management to identify hard drives that are to be monitored and apply threshold settings to those drives. This addresses the issue that there will always be a limited amount of disk space for recordings. The Disk Manager component manages this setting by allowing you to specify one or more drives to host the call buffer and the size of the threshold. This threshold determines when calls will be automatically deleted to make room for newer recordings. Disk Manager always deletes the oldest call first and then advises you by generating a log file.

You can set up the call buffer location and related disk settings, as well as specify which drives are to be monitored by Disk Manager.

To create disk manager settings:

Access Disk Manager by launching the Recorder Manager from any supervisor workstation, providing you have the necessary user permissions.

1. Click **General Setup > Disk Management > Settings**. The Disk Manager Settings screen displays.
2. Complete fields as follows:

Field	Description
Call Buffer Location	Type the disk drive on which the Recorder's Call Buffer is located, such as D:\Recorder\.
Threshold (MB)	Type the disk space size such as 5700. This means that if disk space falls below 5700 MB the disk manager will start deleting old calls to free up more disk space.

3. Click **Save** to save your settings.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To specify disk drives to be monitored:

Specify one or more disk drives whose specified thresholds will be monitored by Disk Manager. The internal Disk Management Web Services component populates a list of all eligible hard drives that you can monitor. This window lists only drives that are not used for call buffering.

1 In the Recorder Manager, click **General Setup > Disk Management > Drives**. The Monitor Drives screen displays,

2 Click the **Monitor** checkbox beside the drives you wish to be monitored.

To change the Threshold value, click Settings and complete the threshold fields.

3 Click **Save**.

To defragment hard drives:

When the Recorder records calls it stores them on the disk in the Calls Buffer. Since the Calls Buffer is used repeatedly it is possible that over time the disk might become fragmented. To improve I/O throughput and disk performance, occasionally it might be necessary to defragment the disk using standard Windows tools.

The task of defragmenting disks is minimized because disk cluster sizes have been increased to 64 kilobytes to reduce the need to defragment. One issue resulting from larger block sizes is that it means using a 64K disk cluster for the 1-2k **`.xml`** file used for each call's meta-data. If you have a **`.wav`** file that takes up say 10 blocks (that is, 640k @ 3k/s=3.5 minute call) and one block is used for the **`.xml`** file it means that you are potentially using 10% of your disk space on a the small **`.xml`** files. However this is a tradeoff for better disk performance.

1 Shutdown the Recorder as described in Starting and Stopping the Recorder and Components on page 59.

2 Backup the Calls Buffer as described in Backing up and Restoring Contacts on page 226.

3 Use the standard windows tool for defragmenting the disk: **Start > All Programs > Accessories > System Tools > Defragmenter.**

4 Restart the Recorder as described in Starting and Stopping the Recorder and Components on page 59.

Changing the Location of the Call Buffer

Change the location specified at installation of the Recorder's call buffer to allocate a different logical or physical drive for the folder that contains the call buffer, also known as the calls cache. Detailed steps are described in Changing the Call Buffer Location on page 64.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Changing a Serial Number

Change a Recorder's serial number to uniquely identify a Recorder after upgrading from a temporary license or to reflect a change in licensing options. Changing a serial number affects the license key of the Recorder. When you change a Recorder's serial number, all existing contacts from the previous serial number will be unavailable and unable to be retrieved from Search and Replay.

To change a serial number:

1. Obtain a new license key for your Recorder's new serial number, as described in Configuring the Recorder License on page 23.
2. In the Recorder Manager, choose **System > License** and click the License option.
3. Type your new license key and click **Update**. The Recorder's serial number is updated to the new number.

   Calls recorded with the previous serial number cannot be replayed.

4. Restart the Recorder as described in Starting and Stopping the Recorder and Components on page 59.

Managing Agents

When agents and other users are added, removed or need updating - for example, they have moved to a new extension - you must make configuration changes both to the Recorder's voice card channels settings (TDM only) and to the Unify Mapping tables. These changes are described in the following sections

To add a new agent:

1. Log onto Recorder Manager and select **General Setup > Voice Cards > Channels.**
2. Identify the associated channel for the agent and add the Agent ID, Extension and Channel Name fields as described in Updating the Configuration of Voice Card Channels on page 118.
3. Add the agent extension in the Unify mapping tables as described in Adding Extensions on page 225.

To update a moved agent:

When an agent or user moves to a different extension, you must delete the old extension and add the new one by doing this:

1. Log onto Recorder Manager and select **General Setup > Voice Cards > Channels**
2. Identify the associated channel for the agent and delete the Agent ID, Extension and Channel Name fields.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 Add the AgentID, extension and Channel Name under the new channel agent is associated with as described in Updating the Configuration of Voice Card Channels on page 118.

4 Update the agent extension in the Unify mapping tables Adding Extensions on page 225.

To delete an agent:

1 In the Recorder Manager select **General Setup > Voice Cards > Channels.**

2 Identify the associated channel for the agent and delete the Agent ID, Extension and Channel Name fields as described in Updating the Configuration of Voice Card Channels on page 118.

3 Delete the agent extension in the Unify mapping tables as described in Adding Extensions on page 225.

Adding Extensions

Add extensions in TDM environments to associate telephone extensions with the individual channels of the Recorder. You can add extensions directly to the Unify script. For adding extensions in IP environments, refer to Managing Extensions on page 86.

To add extensions:

1 Start the Recorder and all components. Make sure that the Capture Component and Unify are running.

2 Make sure that the Recorder has been assigned a serial number and that all voice cards are configured.

3 Start **CTI Studio** and select **Tables > Table Population Wizard.** Make sure that **Transport** is selected as the protocol (the default is TCP/IP).

If you are using Windows XP, you must select **Named Pipes** to start CTI Studio.

4 From the list of Unify tables displayed choose **Mapping Table** and then choose the **Channel** field on the next screen.

5 Choose **Database Population** on the next screen.

Unify communicates with the Capture Component, and retrieves and displays all the available channels.

6 Type the associated extensions for each of the channels and save the table.

Pruning Contacts

Prune contacts to manage the size of the system database by deleting old calls from the database. The Media Database is never pruned automatically. Pruning is done manually by locating the database, listing recorded calls by date, and deleting the oldest ones according to any organization policies.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Some customers plan to never prune contacts and instead add disk capacity very year or two as the database grows. If you do this, consider upgrading your server every few years to compensate for the increasing size of the database. The end result of failing to prune contacts is a reduction in search and update speed.

Backing up and Restoring Contacts

Backup and restore contacts to manually create a duplicate of all files relating to contacts so that in the event of a disaster you can restore data from the backup so that nothing is lost.

Backing up the Recorder is the process of making an exact copy of both the Recorder configuration and the contacts that have been recorded so far or are in the process of being recorded.

Although you can back up the Recorder's configuration even while the Recorder is recording calls, it is advisable that the data is backed up when the Recorder is in a relatively steady state (i.e. when there are no calls being recorded or when only few calls are being recorded. Restoring the Recorder is the process of duplicating the state of the Recorder from a previous back up. Restoring the state involves restoring both the configuration and the data.

To backup the Recorder:

1 Backup the configuration file as follows:

- Log in to Recorder Manager and choose **General Setup > Export/Import > Export**. Both the serial number and the name of the Recorder display.
- Click **Export**. The exported configuration is saved to a file in the location you specify.

2 Back up the registry settings as follows:

- HKEY_LOCAL_MACHINE\Software\Witness
- HKEY_LOCAL_MACHINE\Software\Microsoft\MSLicensing
- HKEY_LOCAL_MACHINE\System\CurrentContolSet\Services\Unify
- HKEY_LOCAL_MACHINE\System\CurrentContolSet\Services\Unify Communications Director
- HKEY_LOCAL_MACHINE\System\CurrentContolSet\Services\UnifyServiceWatcher

3 Back up the following database(s):

- eWareCalls
- eWareConfig
- Audit
- License
- Media
- NGA_SC

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

4 Backup the Recorder sub folder under the installation path. This includes all the binaries for the various Recorder components, all transient data such as persistent queues, and all configuration files and log files.

To restore the Recorder:

1 Restore the Recorder's configuration as follows:

- Log in to Recorder Manager and choose **General Setup > Export/Import > Import**.
- Specify the location of a previously exported Recorder configuration file. A summary of the configuration that is being imported displays.
- Click **Import**.

2 Restore the following Registry Settings

- HKEY_LOCAL_MACHINE\Software\Witness
- HKEY_LOCAL_MACHINE\Software\Microsoft\MSLicensing
- HKEY_LOCAL_MACHINE\System\CurrentContolSet\Services\Unify
- HKEY_LOCAL_MACHINE\System\CurrentContolSet\Services\Unify Communications Director
- HKEY_LOCAL_MACHINE\System\CurrentContolSet\Services\UnifyServiceWatcher

3 Restore eWare database(s) by restoring the following databases onto the new database server:

- eWareCalls
- eWareConfig
- Audit
- License
- Media
- NGA_SC

4 Restore binaries and other transient data by restoring the binaries and transient data from the back-up.

Duplicating (Cloning) and Combining Recorders

This section describes scenarios in which you can duplicate or combine a Recorder. The duplication of a Recorder might be necessary if an existing Recorder has to be migrated onto a new host for performance or reasons such as outdated hardware. Duplicating/cloning preserves the configuration and data of the Recorder.

To duplicate a Recorder and database server that are on the same machine (single-box configuration):

1 Back up the existing Recorder as described in To backup the Recorder: on page 226.

2 Move the voice cards and trunks onto the new machine.

3 Install the Recorder software on the new machine.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

4 Restore the Recorder on the new host as described in To restore the Recorder: on page 227.

To duplicate a Recorder and database server on different machines:

1 Back up the existing Recorder as described in To backup the Recorder: on page 226. Do not backup the system databases).
2 Move the voice cards and trunks onto the new machine.
3 Install the Recorder software on the new machine.
4 Restore the Recorder on the new host as described in To restore the Recorder: on page 227. Do not restore the system databases).

Swapping the System Database

For performance or capacity reasons it might be necessary to swap or migrate database servers to a different, more powerful host. When such a move is necessary, you can migrate the Recorder's system databases onto the new database server.

To swap the system database:

1 Stop the Recorder components as described in Starting and Stopping the Recorder and Components on page 59.
2 Back up the databases as described in Backing up and Restoring Contacts on page 226.
3 Install the database server on the new host/machine.
4 Restore the databases onto the new database server.
5 Start the Recorder components as described in Starting and Stopping the Recorder and Components on page 59.
6 Log in to the Recorder Manager and choose **General Setup > Database Settings.**
7 Edit the existing database entries to reflect the new Database Server.
8 Restart the Recorder components as described in Starting and Stopping the Recorder and Components on page 59.

Performing Oracle Database Maintenance

Perform Oracle database system maintenance to ensure that the Table Space size is adequate and to optimize performance.

To perform Oracle database maintenance:

- **Verify the Table Space size on a regular basis.** As the volume of records in the database increases the table space may reach the Max Size set by default. The max size should be increased when any of the Table Space occupies more than 85% of the space.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- **Set the initial Table Space size.** The initial Table Space size may be too small for long term optimized performance. It is recommended that the initial Table Space size be set to 6 GB.
- **Monitor server performance regularly.** You should monitor the performance of the Oracle Server on a regular basis to ensure optimal performance at all times.

Configuring Oracle Memory (BPMAINDB only)

Configuring Oracle Memory (BPMAINDB only)

Tuning the way that Oracle uses memory can be a complex subject. The following paragraphs provide a brief introduction to how Oracle utilizes memory and also the importance of memory tuning and monitoring. This section applies only to the **BPMAINDB** database if Enterprise Manager is deployed and does not apply to eWare, Balance or WFM using Oracle.

Oracle uses memory segmented into various buffers in order to cache information, instructions, and data. These buffers exist in RAM and in virtual memory and are in place to help the performance of the system in general. It is best to contain all buffers in RAM by setting the LOCK_SGA parameter in the init.ora file. When the buffers spread into the virtual memory, then very intensive memory swaping into and out of the virtual memory space can cause severe I/O bottlenecks and degrade server performance to an unacceptable level. The goal of the buffers is to service as many of the requests as possible. If something can be accessed from the buffers rather than disk storage, then I/O is reduced and the user experience is better overall due to a streamlined service of data and requests.

In buffer tuning and management there is a limit to the size of the buffers, and there is even a point where the buffers can become so large that they are actually detrimental to performance. However this depends on the system in question. In addition to tuning the buffers to CPU, RAM, and I/O activity, you must tune the buffers in relation to each other. Some buffers require the proper sizes on other buffers to perform at optimal speed. The separate buffer areas are:

- The Database Buffer Cache: This buffer contains database object data such as table and index rows for fast access in RAM, therefore reducing I/O.
- The Shared Pool: This buffer contains highly shareable information such as database metadata and parsed SQL code.
- Session Connection Buffers: Every database connection creates a session. Shared memory areas are allocated to each session both within the shared pool and the large pool depending on the configuration.
- The Large Pool: This buffer area is less structured than the shared pool, but services the same type of functions.
- The Java Pool: Used for the Oracle JVM.

All of these areas together are known as the System Global Area, or SGA. You can obtain general SGA information from SQL*Plus by issuing SHOW SGA; You can obtain more information on the SGA by looking at system metadata. The V$SGASTAT view provides some good information on performance and buffer areas.

```
COL name format a32;

SELECT pool, name, bytes
```


© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

```
FROM sys.V$SGASTAT
WHERE pool is null
OR pool = 'large pool'
OR (pool = 'shared pool'
AND (name in ('dictionary cache', 'enqueue', 'library cache',
'parameters', 'processes', 'sessions', 'free memory')))
ORDER BY pool DESC NULLS FIRST, name;
```

As stated before, it is best to try to make the SGA fit into physical RAM and keep it out of virtual memory, however not all systems have enough physical RAM to accommodate the entire SGA.

For more detailed information on Oracle memory tuning and detailed explanations on the structure, architecture, and how to tune each buffer, refer see *http://technet.oracle.com* and download their free documentation library.

Performing Hardware Maintenance

Troubleshooting

Performing Oracle Database Maintenance

Workflow Postgres Database Maintenance

The Postgres database is presently maintained by a software component called Maintainer, which runs as a service and is installed in the workflow folder. The type and schedule of the database maintenance is specified in the MaintainerConfig.xml file stored in the same folder as the Maintainer's executable. A typical MaintainerConfig.xml is shown in the following example:

```
?xml version="1.0" encoding="utf-8" standalone="no" ?>
<maintainer>
    <!-- specifies a duration (in minutes) to wait between
execution of the continuous task the value should be between 1 and
1000 -->
    <ongoing>00:10</ongoing>
    <daily>
        <enabled>true</enabled>
       <!-- timeofday is local time in the format ##:## using a 24
hour clock (i.e 13:30 instead of 1:30 PM)-->
       <!-- set to 3 am as default to be a likely lull in activity
for the Recorder.  -->
        <!-- Doing 3 am to avoid tempting fate with regards to
daylight savings -->
        <timeofday>03:00</timeofday>
    </daily>
```


© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

```
    <weekly>
        <enabled>true</enabled>
        <!-- values are [0..6] where Sunday=0 and Saturday=6 -->
        <dayofweek>0</dayofweek>
       <!-- timeofday is local time in the format ##:## using a 24
hour clock (i.e 13:30 instead of 1:30 PM)-->
       <!-- set to 3 am as default to be a likely lull in activity
for the Recorder.  -->
        <!-- Doing 3 am to avoid tempting fate with regards to
daylight savings -->
    <timeofday>03:00</timeofday>
    </weekly>
    <backup>
        <folder>$APPDIR\workflow\backup\</folder>
        <!-- Assumes postgres is installed under application -->

<utility>$APPDIR\workflow\postgres\bin\pg_dump.exe</utility>
       <!-- This should be set to the destination folder that will
receive copies of the backup -->
        <offline></offline>
    </backup>
    <!-- location of SQL file for reload -->
    <sqlreload>$APPDIR\workflow\sql\wfdbprocs_pg.sql</sqlreload>
</maintainer>
```

To perform on-going maintenance:

The on-going maintenance will perform a vacuuming on all the temp tables.

To perform daily maintenance:

The daily maintenance conducts a single file (**workflow.backup**) backup of the workflow database tables to the **\backup** subfolder in the workflow directory or to the folder specified.

To perform weekly maintenance:

The weekly maintenance performs a system wide vacuum of the entire workflow database.

It is recommended that both daily and weekly maintenance be scheduled at non-busy hours.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To restore a workflow database from a backup:

You can manually restore the workflow database from a backup by using the Postgres Administration utility.

1. In Windows Start menu, go to **Programs > PostgreSQL 8.0 > pgAdmin.**
2. Double-click **Workflow Persistence** and log in using the password of the user account created during installation.
3. Expand **Databases** and highlight workflow.
4. Under Tools, select **Restore** and select the backup file to restore.

To repair a corrupted workflow by reinstalling Postgres:

If the Postgres database is corrupted so that you cannot even start the Postgres database, it may be necessary to reinstall the Postgres database. To reinstall Postgres, the service engineer needs to obtain the ReinstallPostgres.zip file and follow the steps below:

1. Uninstall Postgres using Windows "Add or Remove Programs" Tool.
2. Delete the Postgres folder under Workflow folder
3. Back up the Data and SQL folder containing data of workflow tablespace and SQL files, in case the data is still usable.
4. Delete the Data folder
5. Create a **`C:\workflow`** folder and unzip the files in ReinstallPostgres.zip into that folder.
6. Follow the instructions in the Readme.txt file.

See also the Workflow installation troubleshooting issue Workflow (Postgres) Not Installed on page 237.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Troubleshooting

Troubleshoot your recording system to ensure complete understanding of any problems that might occur and that you can react to them quickly and efficiently. Troubleshooting is divided into hardware and software, as described in the following topics:

- Troubleshooting Hardware Issues
- Troubleshooting Software Issues

Troubleshooting Hardware Issues

Perform hardware troubleshooting to identify and resolve problems with hardware components. This includes checking voice cards, wiring, and system performance to isolate causes and take corrective and preventive action. This information is described in the following topics:

- Checking Voice Cards
- Checking Wiring
- Checking Recorder Performance/Status

Checking Voice Cards

Check voice cards to make sure that the voice card has been recognized by the Recorder and is properly installed and initialized. You can do this at two levels: 1. The voice card Identify feature, which helps in identifying a specific physical card based on its slot and bus number, and 2. At the operating system level, where the Ai-Logix SMARTView tool can be used to recognize the card and make sure that it has been initialized properly.

To check voice cards:

1. Log in to Recorder Manager and click **Alarms** to see if any voice card added/removed alarm(s) have been triggered.
2. Choose **General Setup > Voice Cards**. The pane on the left displays the slot number and bus number for all the cards that have been recognized by the Recorder. Review valid statuses in Changing Voice Cards/NICs on page 215.
3. Select the card that needs to be Identified and then click **Identify**.
4. Do one of the following:

- Look for a flashing LED light on the back of the PC. If the card is properly installed and initialized the capture component communicates with the card and triggers a blink card operation that results in the LED on the card flashing.

It might be necessary to remove the chassis cover to view the LED.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- Launch the appropriate software tool (which accompanies the voice card) to check the card. If the card(s) of interest is not visible on the Voice Cards Tab, then it is possible that the Recorder did not recognize the card.

All voice cards should also be visible in the device manager under windows.

Checking Wiring

Wiring changes for Trunk and Extension tapping are necessary when there are any hardware changes such as adding, removing and replacing voice cards in the Recorder. Wiring changes include replacing input cables and wires into the card from telephone tapping sources.

In all the following scenarios you can use the Ai-Logix SmartView Tool to detect if there are any **Framer Errors** on the card. **Framer Errors** occur when time synchronization is lost between the local clock and the start of a frame signal. In addition to any loss of signal, the Recorder's Capture components raise a loss of signal alarm.

Suggested cable lengths for T1 and E1 DP cards are 15 meters (52 feet) and 30 meters (98 feet) respectively from the tap to the card. For wiring diagrams refer to the Ai-Logix documentation.

To add a new voice card:

1. Restart the Capture Component and let it detect the newly added card.
2. Log onto Recorder Manager and select **General Setup > Voice Cards** and configure the card as described in Changing Voice Cards/NICs on page 215.
3. Make sure the Card has been initialized properly and identify the card with in the host as described in Checking Voice Cards on page 233.
4. Plug in the wiring/cables into the voice card you just added.

Refer to the appropriate card documentation to ensure that a crossover cable is not required.

5. Add the associated extensions as described in Adding Extensions on page 225.

To replace an existing voice card:

1. Restart the Capture Component and let it detect the replaced card.
2. Log onto Recorder Manager and select **General Setup > Voice Cards** and configure the card as described in Changing Voice Cards/NICs on page 215.
3. Make sure the card has been initialized properly and identify the card with in the host as described in Checking Voice Cards on page 233.
4. Copy the configuration from the removed card onto the replaced card.
5. Delete the removed card.
6. Plug in the wiring/cables into the voice card that was replaced.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

To remove an existing voice card:

1. Restart the Capture Component and let it detect the removed card.
2. Log onto Recorder Manager and select **General Setup > Voice Cards** and configure the card.
3. Delete the configuration of the removed card from the capture configuration as described in Deleting a Voice Card on page 114.
4. Copy the configuration from the removed card onto the replaced card.
5. Delete the associated channels from the Unify Mapping table using CTI Studio.

To move an existing voice card:

1. Restart the Capture Component and let it detect the moved card.
2. Log onto Recorder Manager and select **General Setup > Voice Cards** and configure the card.
3. Make sure the card has been initialized properly and identify the card with in the host as described in Checking Voice Cards on page 233.
4. Copy the configuration from the **Removed** instance of this card onto the **Newly Added** instance of this card.
5. Plug in the wiring/cables into the voice card that was moved.
6. Delete the removed card.

Checking Recorder Performance/Status

Check a Recorder's status to view a snapshot of the current performance of the Recorder in terms of alarms raised and pending, the state of archive drives, the state of hard drives that are being monitored, license, and other details about calls. For general computer state and performance measurement such as disk input and output, CPU load, refer to other tools supplied by the Windows operating system or to tools and specifications supplied by other manufacturers.

To check a Recorder's status:

1. Login to the Recorder Manager and choose **Status > Status Summary**. Details of the Recorder's status display.
2. Review the following settings and take any necessary corrective action:

- State (percent full) of Archive drives
- State of hard drives (percent full) being monitored.
- List of active alarms, if any.
- Number of calls in progress.
- Total calls recorded
- Number of unrecorded calls
- Calls per hour.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

For detailed information, refer to Starting and Stopping the Recorder and Components on page 59.

Troubleshooting Software Issues

Perform software troubleshooting to identify and resolve problems resulting from software issues, such as an improperly configured XML file, finding lost calls, and reviewing switch reports. This information is described in the following topics:

- Finding Lost Calls
- Using the Switch Report
- Workflow (Postgres) Not Installed
- Activity Auditing

Finding Lost Calls

Find a lost call to recover data on a call that has been received at the switch but does not display in Search and Replay. Tracing for the lost call should be done in the reverse order of the call life cycle. The life cycle of a call is summarized as follows: **Switch > CTI Logs > Capture Logs > Workflow Database > Consolidator Logs > System Database > Viewer.** Finding a lost call involves starting with a search of the Search and Replay and then working back.

To find a lost call:

1. Gather as much information as available about the missing call, such as approximate time the call was received, extension, agent, channel, and trunk.
2. Prepare a **Query** in Search and Replay with the above information and retrieve the contact. For more information, refer to the *Viewer Installation Guide*.
3. If the call is not found in **Search and Replay**, check the system database **`tblCalls`** (using the call attributes) to verify if the call has been consolidated.
4. If the call is not found in the system database, check the **Consolidator** logs and **Windows Event** logs for any errors. **Consolidator** posts an entry to the **Windows Event** log if there is any problem consolidating a call.
5. If there are no errors in the consolidator log, check the callsbuffer in the **Workflow** database.
6. If the call is not found in the **Workflow** callsbuffer table, check the Recorder online callsbuffer for the **`.wav`** file and the associated call meta-data (**`.xml`**) file(s).
7. If the call is not found in the online callsbuffer check in the **Capture** component logs.
8. If the call is not found in the **Capture** component logs check for the call in the **Unify Source** logs
9. If the call is not found in the **Unify Source** logs check for the call in the **Switch** call logs.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Using the Switch Report

Compare the switch report, which differs by switch manufacturer, to review and compare calls received at the switch and the calls actually recorded by the Recorder. You can then determine if there is any mismatch.

> The switch count of the calls may differ from the Recorder's count of calls as some calls, such as attempted calls, are counted on the switch but not on the Recorder. Similarly conference calls are counted differently on the switch and Recorder.

To compare a switch report:

1. Generate a switch report and capture all the calls received at the switch for a particular time range.
2. Create a query in Search and Replay to retrieve all the calls recorded by the Recorder during the same time range.
3. Compare and identify if there is any mismatch and track the lost calls as described in Finding Lost Calls on page 236.

Workflow (Postgres) Not Installed

In some cases, the Workflow component (PostgreSQL 8.0) is not installed due to a user permissions issue. The problem may occur when, after installing the Recorder the PostgreSQL 8.0 component required for Workflow is somehow not installed on the system.

> You can verify PostgreSQL 8.0 is installed if the **PostgreSQL 8.0** program group exists on the Start Menu.

The cause of this problem is that PostgreSQL 8.0 is installed through an unattended MSI package during installation. The Recorder's InstallShield creates the **`WorkflowAccount`** if it does not exist and grants it rights to log on as a service to run the PostgreSQL processes.

During the installation process the PostgreSQL **`INITDB`** process is executed using the **`WorkflowAcount`**. This account must have the Windows permissions to log on locally for the **`INITDB`** process to be executed. However, the **`INITDB`** process may end the entire PostgreSQL installation will be rolled back (uninstalled) for one of the following reasons:

1. The **`WorkflowAccount`** CANNOT be a member of the built-in "Administrators" or "Power Users" group because PostgreSQL prohibits it.
2. If the system is being installed on a server that is a member of a domain and the security policy of the domain prohibits members of the built-in group "Users" to log on locally the **`INITDB`** process will fail and the PostgreSQL installation will be rolled back.
3. The **`WorkflowAccount`** must have execute permissions on the file **`<windir>\system32\CMD.EXE`**. If the account does not have execute permissions

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

then the **INITDB** process will fail with an access denied error and the installation will be rolled back.

Resolution to Reason #1:

Remove the **WorkflowAccount** from the Administrators or Power-Users group.

Resolution to Reason #2:

Modify the Local Security Policy of the Windows Server to assign the **WorkflowAccount** the permission to log on locally by following these steps:

1. From the Control Panel click **Administrative Tools > Local Security Policy**
2. Click Local Policies > User Rights Assignment > Allow log on locally
3. Add the **WorkflowAccount**. Ensure this assignment is not overridden by the Domain Policy.

Resolution to Reason #3:

Navigate to the System32 folder in Windows Explorer and assign the execute permission to the **WorkflowAccount** to the file **CMD.EXE**.

Activity Auditing

Many user activities are reported in the Recorder to allow you to track and audit configuration changes. These changes appear in log files from the Recorder Manager, from Search and Replay, from trace logs, alarms history, and Windows event viewer. This information may be useful for troubleshooting purposes or can be periodically reviewed and monitored.

To review audit logs from Recorder Manager:

Recorder Manager audits all the user operations performed (except for data retrieval) and provides ability to search and view those events.

1. Login to the Recorder Manager and click **System > Log Viewer**
2. Review the *Severity* section of the log viewer.

To audit Viewer logs

All the retrieve and replay related activities are logged into the Audit database in the Search and Replay application.

1. Login to the Search and Replay application and click **Audit**.
2. Search and review the audit logs that display, as described in Search and Replay's documentation.

To examine trace logs:

Each of the Recorder components has its own log files into which it outputs the trace/log/error/warning messages. This can also be viewed using the Component logs

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

in Recorder Manager. The LogManager utility sets the size of these log files and limits the number of days of log information to be retained, after which it would be replaced by newer files (that is, roll over). Log files are available in the log files sub-folder of the installation folder in zip format (to conserve file space).

Component	Log File
Alarmer	Alarm_<Date>.log
Archiver	Archiver_<Date>.log
Consolidator (CallsConsolidaton)	CallsConsolidator_<Date>.log
DiskManager	DiskManager_<Date>.log
Capture Component	ERecAudioSvc_<Date>.log
Live State Component	LMState_<Date>.log
Consolidator (MediaConsolidation)	MediaConsolidator_<Date>.log
WSFRouter	WSFRouter_<Date>.log

All the components use the standard logging mechanism, in which each entry in the log file is of the form.

<component><module><threadID><DateTime><TextMessage>

The following is an example from Capture Component's log:

[Service|WTelephony|03F0|I] 2005/07/19 00:00:04:484 ECordSync(eRecorderSync) - initialization complete

To review alarm history:

Alarm history contains the history/log of some of the events that the Recorder components have triggered and logged.

1. Log on to Recorder Manager and click **Alarms > Alarm History**.
2. Review the alarms and events of interest that were raised by the Recorder components.

To review Windows' event viewer:

Certain messages are logged into the Windows event log. In addition each Alarm is also logged into the Event Viewer.

1. Access the Windows event log by clicking **Start > Control Panel > Administrative Tools.**
2. Review events related to Recorder.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Appendices

The following topics are included as appendices:

- Compatible Voice Cards
- Alarms Summary
- Using the Diagnostics Tools
- Correcting Checksum Mismatches
- Configuring Integration Service CTI Adapters

Compatible Voice Cards

The following voice cards are compatible with the Recorder.

Type	Ai-Logix Model*	Description
Analog Station Side	**PT409, PT809, PT1609**	Voice cards capable of recording 4, 8, and 16 ports respectively. These cards are currently supported by ContactStore Express and are supported for backwards-compatibility with those customers. They do not generate a loss of signal (LOS) alarm.
	LD409, LD809, LD1609, LD2409	Newer versions of Ai-Logix's analog station-side recording voice cards capable of recording 4, 8, 16, and 24 ports respectively.
Digital Station Side	**NGX800 NGX800-eh**	Voice card that records 8x2-wire digital stations (4x4-wire). It is triggered by D-channel events. It can have up to two MX80 daughterboards attached.
	NGX1600 NGX1600-eh	Voice card that records 16x2-wire digital stations (8x4-wire). It is triggered by D-channel events. It can have one MX80 daugtherboard attached.
	NGX2400 NGX2400-eh	Voice card that records 24x2-wire digital stations (12x4-wire) triggered by D-channel events.
	MX80	Daughterboard that can be installed on NGX800 and NGX1600 voice cards.
Digital and Analog	**DSC-16-PCI DSC-xP-PCI (Cybertech)**	Voice cards from Cybertech that record 16 digital channels (DSC-16) and modular tapping (DSC-xP), which allows inserting analog and digital detection devices (that is daughterboards) into a blank Cybertech motherboard. These show as **16-PCI** and **P-PCI**.
Digital and Analog	**DSC-16-PCI DSC-xP-PCI (Cybertech)**	Voice cards from Cybertech that record 16 digital channels (DSC-16) and modular tapping (DSC-xP), which allows inserting analog and digital detection devices (that is daughterboards) into a blank Cybertech motherboard. These show as 16-PCI and P-PCI.
Digital Trunk Side	**DP3209 DP3209-eh DP6409 DP6409-eh**	Passive-tap recording voice cards capable of recording 30 (DP3209) and 60 (DP6409) channels. They are software switchable between E1 and T1 trunk spans.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Type	Ai-Logix Model*	Description
	PCM3209 **PCM6409**	Passive-tap recording voice cards capable of recording 32 (**PCM3209**) and 64 (**PCM6409**) channels. These cards use the PCM32 protocol, which is similar to E1 in that they are cabled over twisted pair cable and terminated with RJ-45 connectors.
See also: http://www.ai-logix.com and http://www.parrot-dsc.com (Cybertech). **Notes**: 1. NGX 800 appears in Windows Device Manager regardless of NGX card model. 2. **-eh** refers to PCI express card versions. *Except where otherwise noted.		

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Alarms Summary

The following is a summary of all Recorder alarms. The component from which the alarm is triggered is shown under **Category**. The full message, which contains a complete alarm description and troubleshooting guidelines for each alarm, as displayed in Recorder Manager or Enterprise Manager, appears under **Message**. Square brackets [ ] contain variable information extracted from the application. Square brackets can contain text, such as host, or the # symbol, indicating a number. IF is an acronym for Integration Framework. IS is an acronym for Integration Service, which contains the IF.

Short name for UI display	Category	Summary	Message
Archive Media Nearly Full	Archiver	Achiving media is almost full.	Achiving media on [host] is almost full. New media is required soon.
Archive Media Full	Archiver	Archiving media is full.	Archiving media on [host] is full. New media is required immediately.
Archive Lack Media	Archiver	Archiving is stopped due to lack of usable media.	Archiving on [host] is stopped due to lack of usable media. Please check the media in the drive(s).
Archive Format Error	Archiver	Archiving ncountered a format error.	Archiving ncountered a format error on [host].
Archive DB Error	Archiver	Archiver cannot connect to the database.	Archiver on [host] cannot connect to the database on [DB server name or net service name]. [error description]. Please check the network connection and database.
Archive Behind	Archiver	Archiver is behind for a recorder	Archive against recorder [recorder] from drive [device name] on server [host] is behind by [number] day(s).
Archive File Error	Archiver	Archiver is unable to access the file.	Archiver on [host] is unable to access file [file name]. Please check the file authorization.
Archive DB Queue	Archiver	Threshold has been crossed for Archive DB queue.	The size of the queue holding archive updates on [host] for the media database is above its threshold. The current queue size is [#] and the threshold is [#].
Archive File Not Found	Archiver	A target file could not be located for archive.	An unarchived file, [file name] could not be located from [host]. Some recorded data may be lost.
Archive Drive Missing	Archiver	Archive drive missing.	One or more configured archive drives on [host] are no longer present-. Please check the physical drives and/or reconfigure.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Archive Drive Deleted	Archiver	New archive drive(s) were detected.	New possible archive drives detected on [host] - if you wish to use them, please reconfigure Archiver.
Archive Write Error	Archiver	Archiver encountered a "write" error.	Archiver on [host] failed to write to medium. The medium may be corrupted.
Archive Drive Not Clean	Archiver	Archive drive requires cleaning.	Archive drive [drive name] on [host] requires cleaning.
Archive Read Only Medium	Archiver	A read-only medium for archiving has been detected	A read-only medium, [drive name], for archiving on [host] has been detected.
Archive Error	Archiver	Archiver encountered a system error.	Archiver on [host] encountered a system error. [error description].
Archive Fetch Error	Archiver	Enterprise Archiver encountered an error while fetching a file.	Archiver on [host] was unable to fetch a file. [error description]
Archive Media Failure	Archiver	An error was encountered on an Archive medium	Archiver on [host] encountered a media failure. [error description]
Archive Replay Failure	Archiver	Archiver was unable to replay from media	Archiver on [host] was unable to replay from archive media. [error description]
Archive Database Timeout	Archiver	Archiver encountered a database timeout error.	Archiver on [host] encountered a database timeout while executing '[function]'. [error description]
Archive Database Error	Archiver	Archiver encountered a database error.	Archiver on [host] encountered a database error while executing '[function]'. [error description]
Disk Min Space Reached	Disk Manager	Free disk space has reached the minimum.	Free disk space on drive [drive] of [host] has reached the minimum of [threshold] MB. Please free unused disk space on the drive.
Disk Full	Disk Manager	No more disk space is available.	No more disk space available on drive [drive] of [host]. Please free unused disk space on the drive.
DiskManager Delete Failed	Disk Manager	Disk Manager failed to delete file.	Disk Manager on [host] can not delete file [file name]. Please check the file authorization.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Disk Manager Deleted Un-Archived File	Disk Manager	Disk Manager deleted a file that was not archived.	Disk Manager on [host] deleted file [file] before it was archived. Please verify your archive solution.
Disk Manager Detected Un-Archived File	Disk Manager	Disk Manager detected a file that was not archived.	Disk Manager on [host] detected files [files list] that were not archived after [num days] days. Please verify your archive solution.
Invalid License	Capture, ScreenCapture	The license for Capture is invalid.	The license for Capture on [host] is invalid A new license is required.
License About To Expire	Capture, IPCapture, ScreenCapture	The license for Capture is about to expire.	The license for Capture on [host] has about to expire. Please renew your license as soon as possible.
License Expired	Capture, IPCapture, ScreenCapture	The license for Capture has expired.	The license for Capture on [host] is expired. A new license is required.
License Key Missing	Capture, IPCapture, ScreenCapture	License key is missing.	License key is missing on [host].
Card Changed	Capture	Voice card is added or removed or replaced.	Voice card is added, removed or replaced on [host]. The card type is [card type] and the card serial number is [card serial number].
Card Initialization Error	Capture	Failed to initialize voice card.	Failed to initialize voice card on [host] due to [failure reason]. If the failure is due to firmware corruption, you need to either replace the card or disable the card temporarily. For other types of failures, you may need to reboot the system to correct the problem.
Channel Initialization Error	Capture	Failed to initialize channel.	Failed to initialize channel [channel id] on [host].
Capture File Error	Capture, IPCapture	File error from Capture.	File error from Capture on [host] for [file name]. [Error description].
Recording Error	Capture, ScreenCapture	An error occurred during recording.	An error occurred during recording for call [INUM] and channel [logical channel id] on [host]. [Error description].
LOS Event	Capture	TDM Recorder (ITS IP Recorder) received a Loss Of Signal (LOS) event.	The TDM Recorder (ITS IP Recorder) on [host] has received a Loss of Signal (LOS) alarm for board serial # [serial #], framer [framer #], channel [logical channel id]. Please check the telephony cabling.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

LossOfFrame	Capture	TDM Recorder (ITS IP Recorder) received a Loss of Frame alarm.	The TDM Recorder (ITS IP Recorder) on [host] has received a Loss of Frame alarm for board serial # [serial #], framer [framer #], channel [logical channel id]. This may be due to incorrect frame setting. Please check the card configuration.
Fallback Entered	Capture	Capture entered fallback recording mode.	Channel [channel id] on [host] entered fallback recording mode.
Channel State Mismatch	Capture	A channel state mismatch has been detected	Channel State mismatch for channel [Channel id] on recorder [recorder host] is detected. Calls on this channel may seem to start late or appear to have the wrong voice. Please check the physical wiring and recorder configuration such as VOX settings, protocol, PBX Type, inbound and outbound idle code and the Unify mapping table.
Channel Command Queue	Capture	Threshold is crossed for ChannelCommandQueue.	The size of the queue holding total channel jobs on [host] is above its threshold. The current queue size is [#] and the threshold is [#].
Consolidator DB Connect Error	Consolidator	Consolidator cannot connect to database.	[Media/Calls Consolidator] on [host] cannot connect to database on [DB server name or net service name]. [error description].
Consolidator Database Error	Consolidator	Consolidator encountered a database error.	[Media/Calls Consolidator] on [host] encountered a database error processing file [file name]. [error description].
Auto Register CapturePlatform Failed	Consolidator	Auto Registration of CapturePlatform has failed.	Consolidator on [host] encountered an error while registering the CapturePlatform. [error description].
Workflow Connect Error	Workflow	Workflow cannot connect to database.	[Component name] Workflow on [host] cannot connect to database.
Workflow Config Error	Workflow	Workflow configuration error.	Workflow on [host] failed to read configuration.
Live Monitor Recorder Error	LiveMonitor	Live Monitor cannot connect to a recorder	The Live Monitor State Service on recorder [Live Monitor Host Name] cannot Connect to recorder [Recorder Host Name]. Please check the network path between the two recorders. Calls from this recorder will not appear in Observer until the connection is restored.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Live Monitor Viewer Error	LiveMonitor	Live Monitor Cannot Connect to Viewer	The Live Monitor State Service on recorder [Live Monitor Host Name] cannot Connect to Viewer to verify restrictions on host [Viewer Host Name]. Please check the network path between the Live Monitor recorder and Viewer. Observer clients will not be able to connect until the connection to Viewer is restored.
System Error	All	A system error occurred.	A system error occurred on [host]. [Exception description].
Encryption Key Warning	All	Cannot obtain encryption key. Processing continues.	[host] was unable to obtain an encryption key. Processing will continue using non-encrypted files. Exception details: [details]
Encryption Key Expired Warning	All	An expired encryption key was retrieved from the local cache.	[host] retrieved an expired encryption key from the local cache. A probable communication error with the KMS should be investigated and corrected. [details]
Encryption Key Error	All	Cannot obtain encryption key. Processing halted.	[host] was unable to obtain an encryption key. Processing will halt until the error is corrected. Exception details: [details]
Success	Alarmer	No alarms are triggered in the past 24 hours.	No alarms are triggered on [host] in the past 24 hours.
Capture Stopped	Capture	Capture is stopped or is unavailable.	Capture on [host] is stopped or is unavailable.
Consolidator Stopped	Consolidator	Consolidator is stopped or is unavailable.	Consolidator on [host] is stopped or is unavailable.
DiskManager Stopped	DiskManager	DiskManager is stopped or is unavailable.	DiskManager on [host] is stopped or is unavailable.
Archiver Stopped	Archiver	Archiver is stopped or is unavailable.	Archiver on [host] is stopped or is unavailable.
Maintainer Stopped	Workflow	Workflow Maintainer is stopped or is unavailable.	Workflow Maintainer on [host] is stopped or is unavailable.
Web Service Stopped	WebService	Recorder Web Service is stopped or is unavailable.	Recorder Web Service on [host] is stopped or is unavailable.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Live State Stopped	LiveMonitor	Live Monitor State Service is stopped or is unavailable.	Live Monitor State Service on [host] is stopped or is unavailable.
Email Error	Alarmer	Failed to send email notification.	Failed to send email notification. Please check the status of Recorder Manager server on [host] and the status of email server on [email server name].
Failed to Send Trap	Alarmer	Failed to send SNMP trap message.	Failed to send SNMP trap message. Please check the SNMP trap configuration on recorder [host] and the trap host status on [trap host name].
Packets Dropped By Driver	IPCapture, IPAnalyzer	There are packets being dropped by the driver on the network adapter.	On [host], there are packets being dropped by the driver on the network adapter [adapter]. The number of packets being dropped by the driver so far is [#]. RESOLUTION: The recorder is seeing too much network traffic and cannot handle the load. This problem might be caused by a network mis-configuration. Have any changes been made to the network, recently? Please check for correct configuration. You may be losing call data because of this problem.
Record Jobs Queue	IPCapture	Threshold has been crossed for Record Jobs Queue.	The size of the queue holding the record jobs in the system [host] has crossed the threshold. The current queue size is [#] and the threshold is [#]. RESOLUTION: Writing to the call buffer hard disk may be slow on the system. This problem might be caused by a system misconfiguration. You may be losing call data because of this problem. Please check for the correct anti-virus software configuration. Refer 'Anti-virus software configuration' section of Installation guide. Also check the call buffer hard disk RAID configuration. Refer 'Storage capacity and location', 'Supported Hardware and Topologies' sections of System Administration Guide.
Workflow Message Queue	IPCapture	Threshold has been crossed for Workflow Message Queue.	The size of the queue holding the messages to Workflow in the system [host] has crossed the threshold. The current queue size is [#] and the threshold is [#]. RESOLUTION: The connection to Workflow data base is down. Please check whether 'Contact Store Workflow Persistence' service is running. You may be losing post call record processing because of this problem.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

IP Packets Per Second	IPCapture	The number of IP packets received per second has spiked.	The number of IP packets received per second on system [host] has seen a spike. The number of packets received per second is [#] and the threshold is [#]. RESOLUTION: The recorder is seeing too much network traffic and cannot handle the load. This problem might be caused by a network mis-configuration. Have any changes been made to the network, recently? Please check for correct configuration. You may be losing call data because of this problem.
Packets Received Per Second	IP Analyzer	The number of IP packets received per second has spiked.	The number of IP packets received per second on system [host] has seen a spike. The number of packets received per second is [#] and the threshold is [#].RESOLUTION: The recorder is seeing too much network traffic and cannot handle the load. This problem might be caused by a network mis-configuration. Have any changes been made to the network, recently? Please check for correct configuration. You may be losing call data because of this problem.
Cable Cross Connected	Capture	Capture receives cable cross connected signal	The TDM Recorder (ITS IP Recorder) on [host] has received a cable cross connected alarm on trunk [trunk #], board [board #]. RESOLUTION: You may need to configure the PRI trunk tap to be crossed over. Please check the telephony cabling.
License Reaching Max Limit	Capture, IPCapture, ScreenCapture	The license of the recorder is approaching its maximum limit.	The recorder on [Host Name] is approaching the licensed channel recording limit. The current number of channels in recording is [Current Rec channel count] and the maximum licensed recording limit is [Total Licensed Channels] channels. The number of calls reached this limit is [Count of calls that reached the limit].
License Max Limit Reached	Capture, IPCapture, ScreenCapture	The capture has reached the maximum license limit.	The recorder on [Host Name] has reached the maximum licensed recording limit. The maximum licensed recording limit is [Total Licensed Channels] channels. No new calls will be recorded until the number of channels in recording goes below the licensed limit. The number of calls that reached this limit is [Count of calls reached the limit].
IPCapture Stopped	IPCapture	IPCapture Engine Service has stopped or is unavailable.	IP Capture Engine Service on [host] has stopped or is unavailable.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Analyzer Stopped	IPAnalyzer	Analyzer Service has stopped or is unavailable.	Analyzer Service on [host] has stopped or is unavailable.
Compressor Stopped	Compressor	Compressor Service has stopped or is unavailable.	Compressor Service on [host] has stopped or is unavailable.
Invalid Configuration File	All	Configuration File is invalid.	Invalid configuration file on recorder [recorder host name] for [component name]. File "[full file path]" is either missing or has invalid configuration. Please correct the configuration and restart the service. If the file is under "…\conf\Cache" directory, you need to set up your configuration in the Enterprise Manager in order for the file to be generated.
No Packets Received	IPCapture, IPAnalyzer	Not seen any traffic on a Network Interface Card.	The [host] has not seen any network traffic on the [local area connection] ([Network Interface Card Identifier]) for more than [duration] seconds.
Pcap Set Buffer Failed	IPCapture, IPAnalyzer	Unable to allocate driver's circular buffer	On [host], [Component] is unable to allocate driver's circular buffer for [AdapterConnectionName] for adapter with ID = [Adapter ID]. [Component] will retry to allocate the buffer. If the problem is persistent and can't allocate the buffer, please restart the [Component] service.
Error Reading Packet	IPCapture, IPAnalyzer	Error while reading packet from Adapter	On [host], [Component] is having a problem to read packets from [AdapterConnectionName] for adapter with ID=[Adapter ID]. [Component] will retry to read the packets. If the problem is persistent and can't read the packet, please restart the [Component] service.
No Enabled Adapters	IPCapture	No enabled Adapters found	On [host], [Component] didn't find enabled adapters to sniff the network. RESOLUTION: Are you using Active Recording mode to record the calls? If not, please enable the Adapters to record and restart the [Component] service. You won't be recording calls as there is no enabled Adapter to sniff the network.
Integration Framework Started	IFService	The Integration Framework has started.	The Integration Framework has started on [host].
Integration Framework Down	IFService	The Integration Framework has stopped.	The Integration Framework has stopped on [host]

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Recorder Controller Started	IFService	The Recorder Controller has started.	The Recorder Controller has started on [host].
Recorder Controller Down	IFService	The Recorder Controller has stopped.	The Recorder Controller has stopped on [host].
Adapter Started	IFService	The Adapter has started.	Adapter [adapter name] has started on [host].
Adapter Link Down	IFService	The Adapter has lost communication with a resource.	Adapter [adapter name] has lost communication with [resource] on [host]. Reason: [reason]..
Adapter Data Error	IFService	The Adapter encountered a Data Error.	Adapter [adapter] encountered a data error processing an event on [host]. Reason: [reason].
Adapter Start Failed	IFService	The Adapter failed to start.	Adapter [adapter name] on [host] has failed to start.
Adapter Shut Down	IFService	The Adapter has stopped.	Adapter [adapter name] on [host] has stopped.
Minor Business Rule Queue Overloaded	IFService	Minor threshold is crossed for Business Rule Queue	The size of the queue holding events for business rule processing on [host] is above its minor threshold. The current queue size is [#] and the threshold is [#].RESOLUTION: Check that your system is sized appropriately for the number of devices that you are recording.
Major Business Rule Queue Overloaded	IFService	Major threshold is crossed for Business Rule Queue	The size of the queue holding total screen channel jobs on [host] is above its major threshold. The current queue size is [#] and the threshold is [#].RESOLUTION: Check that your system is sized appropriately for the number of devices that you are recording.
Minor Business Rule Latency	IFService	Minor latency threshold is crossed for Business Rule processing	The time to process business rules on [host] is above its minor threshold. The current delay is [#] seconds and the threshold is [#] seconds. RESOLUTION: Check that your system is sized appropriately for the number of devices that you are recording.
Major Business Rule Latency	IFService	Major latency threshold is crossed for Business Rule processing	The time to process business rules on [host] is above its major threshold. The current delay is [#] seconds and the threshold is [#] seconds. RESOLUTION: Check that your system is sized appropriately for the number of devices that you are recording.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Minor Recording Latency	IFService	Minor latency threshold is crossed for making recording requests	The time to request CTI-controlled recording on [host] is above its minor threshold. The current delay is [#] seconds and the threshold is [#] seconds. RESOLUTION: Check that your system is sized appropriately for the number of devices that you are recording.
Major Recording Latency	IFService	Major latency threshold is crossed for making recording requests	The time to request CTI-controlled recording on [host] is above its major threshold. The current delay is [#] seconds and the threshold is [#] seconds. RESOLUTION: Check that your system is sized appropriately for the number of devices that you are recording.
Minor NGA Message Queue Overloaded	IFService	Minor threshold is crossed for Recorder Message Send Queue	The size of the queue holding messages to send to [recorder type] Recorder on [host] is above its minor threshold. The current queue size is [#] and the threshold is [#]. RESOLUTION: Check that your system is sized appropriately for the number of devices that you are recording.
Minor NGA Message Queue Overloaded	IFService	Major threshold is crossed for Recorder Message Send Queue	The size of the queue holding messages to send to [recorder type] Recorder on [host] is above its major threshold. The current queue size is [#] and the threshold is [#].RESOLUTION: Check that your system is sized appropriately for the number of devices that you are recording.
Record Control Type Mismatch	IFService	Record Control Type Mismatch between EM and RM	Device [extension or trunk] in member group [member group name] on switch [switch name] is configured to be controlled by [CTI or Recorder]. Channel [channel] on Recorder [node name] which records this device is configured to be controlled by [CTI or Recorder]. RESOLUTION: Recording will be controlled by [CTI or Recorder]. Please update your configuration so that these settings match.
Device Association Conflict	IFService	Agent logged into device that conflicts with configured device association	Agent [agent Name] has logged in to device [device] which conflicts with the configured phone [extension] and workstation [workstation] association. RESOLUTION: Correct the device association conflict in Enterprise Manager by either updating the phone and workstation association to include the correct devices or by removing the association between the devices if the phone and workstation association is not static.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

BT Routiner Error	IFService	The BT Recorder Line Routiner has encountered an error.	The BT Recorder Line Routiner has encountered an error on [host name] where [error reason].
Recorder Disconnected From IS	IFService	Recorder is disconnected from Integration Service	Recorder <host name> Disconnected From Integration Service < host name >
Connection Lost To Primary IS	IFService	Connection has been lost to the primary IS	Primary Integration Service <host name> Disconnected From Secondary <host name>
Connection Lost To Secondary IS	IFService	Connection has been lost to the secondary IS	Secondary Integration Service <host name> Disconnected From Primary <host name>
TDM Recorder (ITS IP Recorder) Unusual Call Volume	Capture	Expected calls recorded are below threshold	Calls recorded on [host] is below the configured threshold. The number of calls recorded in last hour is [#] and the threshold is [#].
IP Recorder Unusual Call Volume	IPCapture	Expected calls recorded are below threshold	Calls recorded on [host] is below the configured threshold. The number of calls recorded in last hour is [#] and the threshold is [#].
Screen Capture Unusual Call Volume	ScreenCapture	Expected calls recorded are below threshold	Calls recorded on [host] is below the configured threshold. The number of calls recorded in last hour is [#] and the threshold is [#].
High Processor Usage	All	Recorder Server is under heavy load	CPU usage on [host] is above threshold. Average CPU usage for last 15 min is [#]% and the threshold is [#]%. If the TDM Recorder (ITS IP Recorder) is installed, please ensure unused or disconnected channels are disabled.
High Processor Interrupts/sec	All	Recorder Server Processor has high Interrupts/sec	"[Interrupts/sec on [host] is above threshold. Average Interrupts/sec for the last 15 min is [#] and the threshold is [#].
High Physical Disk Queue Usage	All	Recorder Server Processor has high Physical Disk Queue Length	Physical Disk Queue Length on [host] is above threshold. Average Disk Queue Length for the last 15 min is [#] and the threshold is [#]
High Memory Usage	All	Recorder Server has high Memory Usage	Memory usage on [host] is above threshold. Average memory usage for the last 15 min is [#]% and the threshold is [#]%

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Screen Capture Stopped	Screen Capture	Screen Capture is stopped or is unavailable.	Screen Capture on [host] is stopped or is unavailable.
Screen Channel Command Queue	Screen Capture	Threshold is crossed for Screen Channel Command Queue	The size of the queue holding total screen channel jobs on [host] is above its threshold. The current queue size is [#] and the threshold is [#].
Agent Capture Unreachable	Screen Capture	Agent Capture is not reachable.	Recorder on [host] can not connect to Agent Screen Capture operating on [agent host name] on port [port #]. Please check the network connection to the agent workstation and ensure the Agent Screen Capture service is running.
No Data Received From Agent Capture	Screen Capture	No data packets have been received from Agent Screen Capture.	Recorder on [host] have not received any data packets for record session [INUM] from Agent Screen Capture operating on [agent host name] on port [port #].
No More Screen Channels Available	Screen Capture	No more screen channels are available for recording	No more screen channels are available for recording on recorder [host]. The configured maximum number of screen channels is [max # of screen channels] and all channels are in use. Please increase the maximum number of screen channels.
File Tampered	All	A file has been tampered with.	On [host], file "[file name]" may have been tampered with. Please refer to the System Administration Guide for details on how to correct a tampered file.
Content Server Stopped	ContentServer	Content Server is stopped or is unavailable.	Content Server on [host] is stopped or is unavailable.
SSL Configuration Error	ContentServer	An SSL configuration error has occurred.	SSL is configured for [component name] on host [recorder host name], but a required file is missing. The file is [file name]. Please deploy the file or remove SSLConfiguration by modifying [SSL configuration parameter].
SSL Failed Connection	ContentServer	An SSL connection has failed.	An SSL connection was attempted on host [host name], port [SSL listen port] but a required file is missing. The file is [missing file for SSL Configuration]. Please deploy the file or remove SSLConfiguration for the client.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Duplicate Packets Received	IPCapture, IPAnalyzer	Recorder has received duplicate packets.	On [host], Recorder has received duplicate [#] packets. The number of duplicate packets received so far is [#]. RESOLUTION: The recorder is seeing duplicate packets. This problem might be caused by a span port mis-configuration. Have any changes been made to the network, recently? Please check for correct span configuration. You may be losing call data because of this problem.
Packets Missed	IPCapture, IPAnalyzer	Recorder has missed packets.	On [host], Recorder has missed [#] packets. The number of missed packets so far is [#]. RESOLUTION: This might be because of network mis-configuration or overloaded network. Have any changes been made to the network, recently? Please check for correct span configuration. You may be losing call data because of this problem.
Call Buffer Free Space Too Low	DiskManager	The amount of free space on the Call Buffer drive has dropped below the given threshold	The Available Disk Space on the Call Buffer Drive of [host] has fallen below the threshold of [#]

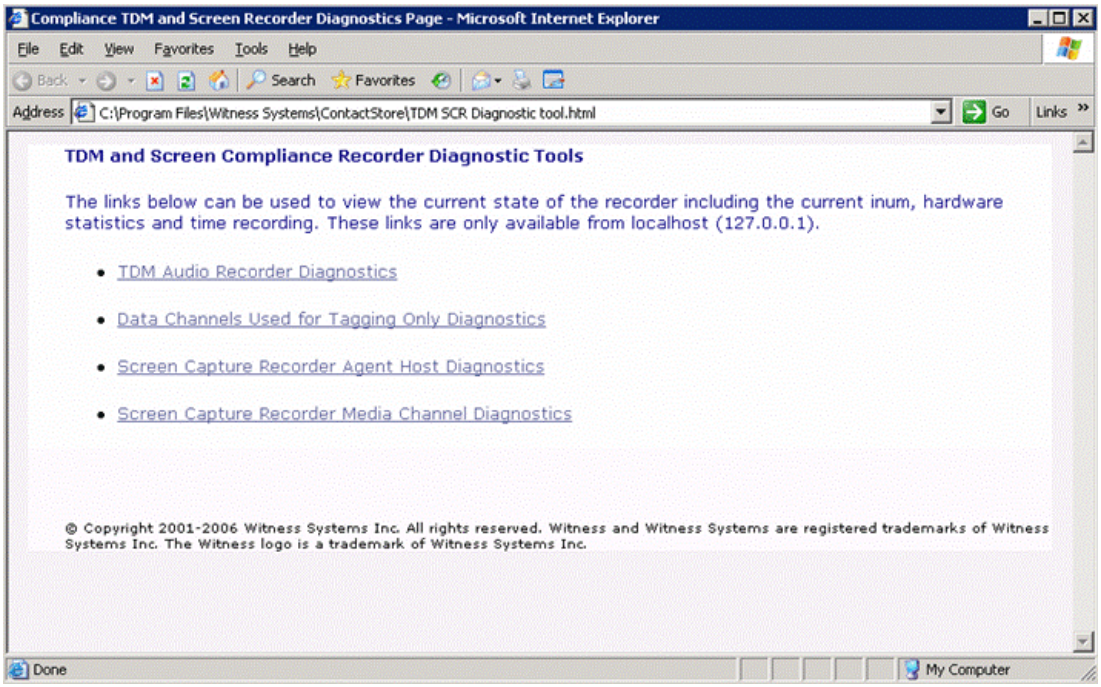
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Using the Diagnostics Tools

Use the diagnostics tools in the Contactstore folder to help with problem solving and troubleshooting by viewing recording activity in a TDM or Screen Recorder without stopping the Recorder. You can view the status of the channels/recordings, see what extensions, screen hosts and INUMS are currently being recorded. On TDM Recorders only, you can see details such as channel voltages and synchronization alarms while the recorder is running.

To use the Diagnostics Utility:

1. Choose **Start > Windows Explorer** and navigate to the Contactstore directory in your Recording system's installation folder (the c:\\ drive by default).
2. Click **TDM SCR Diagnostic tool.html**. The Recorder Diagnostics page displays.


Compliance TDM and Screen Recorder Diagnostics Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Program Files\Witness Systems\ContactStore\TDM SCR Diagnostic tool.html
Go Links
TDM and Screen Compliance Recorder Diagnostic Tools
The links below can be used to view the current state of the recorder including the current inum, hardware statistics and time recording. These links are only available from localhost (127.0.0.1).
TDM Audio Recorder Diagnostics
Data Channels Used for Tagging Only Diagnostics
Screen Capture Recorder Agent Host Diagnostics
Screen Capture Recorder Media Channel Diagnostics
© Copyright 2001-2006 Witness Systems Inc. All rights reserved. Witness and Witness Systems are registered trademarks of Witness Systems Inc. The Witness logo is a trademark of Witness Systems Inc.
Done
My Computer

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

3 Choose a utility according to the following:

Item	Description
TDM Audio Recorder Diagnostics	Allows you to analyze call channel data being captured in a TMD Recorder (ITS IP Recorder), such as channel status, line voltage, VOX details for every channel, and INUMs. Other information includes available number of channels, enabled channels, and mapping between physical channels and media channels. Errors include **Loss of Signal** (LOS) and **Loss of Frame** (LOF). Channel states include **Recording** (the channel is on a call and is being recorded) and **Idle** (the channel is not on a call and is not being recorded by the Recorder).
Data Channels Used for Tagging only Diagnostics	Allows you to analyze the metadata in TDM calls currently being captured.
Screen Capture Recorder Agent Host Diagnostics	Allows you to analyze activities in a screen Recorder on an Agent's PC, including data such as: Hostname, Media Channel number, Current command on the Media Channel, and Last seen INUM.
Screen Capture Recorder Media Channel Diagnostics	Allows you to analyze the metadata currently being captured in a screen Recorder.

4 Close the tool when finished.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Correcting Checksum Mismatches

Correct checksum mismatches as part of a tamperproofing (security) recovery procedure to correct configuration files that have been tampered with. This involves resetting the checksum string, which is inserted for security into all configuration files. Correcting Checksum Mismatches describes recovery procedures for using either Recorder Manager, Enterprise Manager, or a command line utility to correct these files. Information is presented in the following topics:

- Correcting Tampering
- Correcting Tampering from a Command Line

Correcting Tampering

Use Recorder Manager (RM) or Enterprise Manager (EM) to correct configuration files that have been identified, through system alarms, as having been tampered with. All files are tamperproofed automatically. In tamperproofing, a checksum string is inserted into configuration files, allowing the detection and reporting of mismatched checksums. The following table lists the applicable configuration files and how to correct reported mismatches after detection.

When the **Fingerprint** option is selected in Recorder Manager, as described in Configuring Recorder Settings (Call Buffer) on page 62, a checksum string is inserted into **`.wav`** files, allowing the detection and reporting of mismatched audio files.

As system administrator with the goal of resolving the alarm (see the **File Tampered** alarm in on page 243), you use RM or EM to update the checksum in the file, as in the following table.

Mismatched File	**To update the checksum ...**
Recorder configuration files (all XML files in <Witness Install Directory>\ContactStore)	
RecorderGeneral.xml	RM > General Setup > Recorder Settings > Save.
AlarmConfig.xml	RM > Alarms > Alarm Settings or Notification Profile > Save.
ArchiverConfig.xml	RM > Operations > Archive > Save.
DiskManagerConfig.xml	RM > General Setup > Disk Management > Save.
CompressorConfig.xml	RM > General Setup > Compression > Save
ConsolidatorConfig.xml	RM > General Setup > Database Settings > Save
TDMConfig.xml	**1.** RM > General Setup > Voice Card > Save, and **2.** RM > System > License > Save.
IPCaptureConfig.xml	**1.** RM > Operations > Extensions > Save. **2.** RM > General Setup > Network Settings > Save. **3.** RM > System > License > Save.
IPAnalyzerConfig.xml	RM > System > License > Save.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Mismatched File	To update the checksum ...
ScreenConfig.xml	RM > General Setup > Recorder Settings > Save.
LiveStateConfig.XML	RM > System > Live Monitor > Save.
SFIConfig.xml	EM > System > Installation > Security > Save.
Integration Service configuration files (all XML files in <Witness install directory>\conf)	
IFServices.xml	RM > General Setup > Integration Framework > Save.
SecurityConfig.xml	EM > System > Installation > Security > Save.
Data cache files (all XML files in <Witness install directory>\conf\cache)	
Cache-Manifest.xml	EM > Any change that will trigger a data cache update > Save.
datasource-<data source identifier>.xml	EM > System > Data Sources > Save.
recorders.xml	EM > System > Installation > Save.
organization--<organization id>.xml	EM > People > Profiles > Save.
attributes.xml	EM > System > Data Sources > Save.
businessrules.xml	EM > System > Manage Rules > Save.
RM configuration files (all XML files in <Witness install directory>\TomCat5\config\)	
User.xml	RM > System > Manage User > Save.
UserManager.xml	RM > Preferences > Close.
ConfigManager.xml	EM > System > Administration > EM Location > Save.

The following configuration files must be corrected using the ChecksumUtil command line utility, as they cannot be corrected in RM or EM:

- MaintainerConfig.xml
- wsconfig.xml
- RecorderComponentsConfiguration.xml
- ComponentManagementConfig.xml
- IPCaptureProtocolConfig.xml
- MasterConfig.xml
- KMCLocalProviderConfig.xml
- KMCRSAProviderConfig.xml
- RecorderController.xml

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- AdapterData.xml
- LogServerManager.xml
- ListConfigManager.xml
- adapter.xml

Correcting Tampering from a Command Line

Use a command line (that is, a DOS window) to correct tampering, as described in Correcting Tampering on page 259. The following steps describe how to launch a command line utility and how to correct reported mismatches using the command line. Typically, the file that has been tampered with is reported through an alarm. As system administrator with the goal of resolving the alarm (see the **File Tampered** alarm in on page 243), you launch a command line utility and reset the checksum in the file, as in the following steps.

1 Open a DOS window, and navigate to the folder containing the Checksum utility (typically **...Program Files\Witness Systems\ContactStore**).

Note: If you click the .exe file in Windows Explorer, nothing happens.

2 Type **`checksumutil.exe`** followed by one or more of the following parameters:

Parameter	Description
`-gall`	Create the checksum for all files.
`-g <FileName>`	Create the checksum for the specified file.
`-gd <DirName>`	Create the checksums for all the files in the specified directory.
`-vall`	Validate the checksum for all files.
`-v <FileName>`	Validate the checksum for the specified file.
`-vd <DirName>`	Validate the checksums for all the files in the specified directory.

For example, to correct the checksum string in the file AlarmConfig.xml you would type the following in the DOS window:

`checksumutil -v <AlarmConfig.xml>`

If XML file is in a different directory you need to give complete path details, such as **`checksumutil -v <path to XML file ... /AlarmConfig.xml>`**.

The ChecksumUtil utility corrects only .xml files.

A list of all parameters is displayed on the screen when you type **ChecksumUtil.**

The checksum digit in the specified configuration file(s) is corrected.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Configuring Integration Service CTI Adapters

Configure CTI adapters to apply specific settings to each adapter so that it can be used with the Recorder's Integration Service. The Integration Service relays information from the adapter to the Recorder. Select the adapter in the left-hand pane and click the Start or Stop buttons to start and stop the adapter. Choose a CTI adapter from the following list:

Alcatel

- Alcatel Omni PCX 4400 via TSAPI

Aspect

- Aspect Event Bridge
- Concerto for Aspect Unison/Ensemble/Ensemble Pro
- Aspect Contact Server (Portal)

Avaya

- Avaya Definity G3/S8x00 via TSAPI
- Avaya DLG Adapter
- Avaya PDS 12 and 3.0
- Avaya ASAI via CVLAN Adapter

British Telecom

- BT Integration

Cisco

- Cisco CallManager with JTAPI
- Cisco Call Manager

Genesys

- Genesys Adapter

Nortel

- Nortel Meridian/Succession via CTConnect
- Nortel Meridian/Succession via MLS

ICM (for Avaya, Cisco Call Manager, or Cisco IP)

- Cisco CallManager with JTAPI

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

eQuality Connect

- eQuality Connect

Exec Record

- Exec Record and TCP/IP API/Unify

Alcatel Omni PCX 4400 via TSAPI

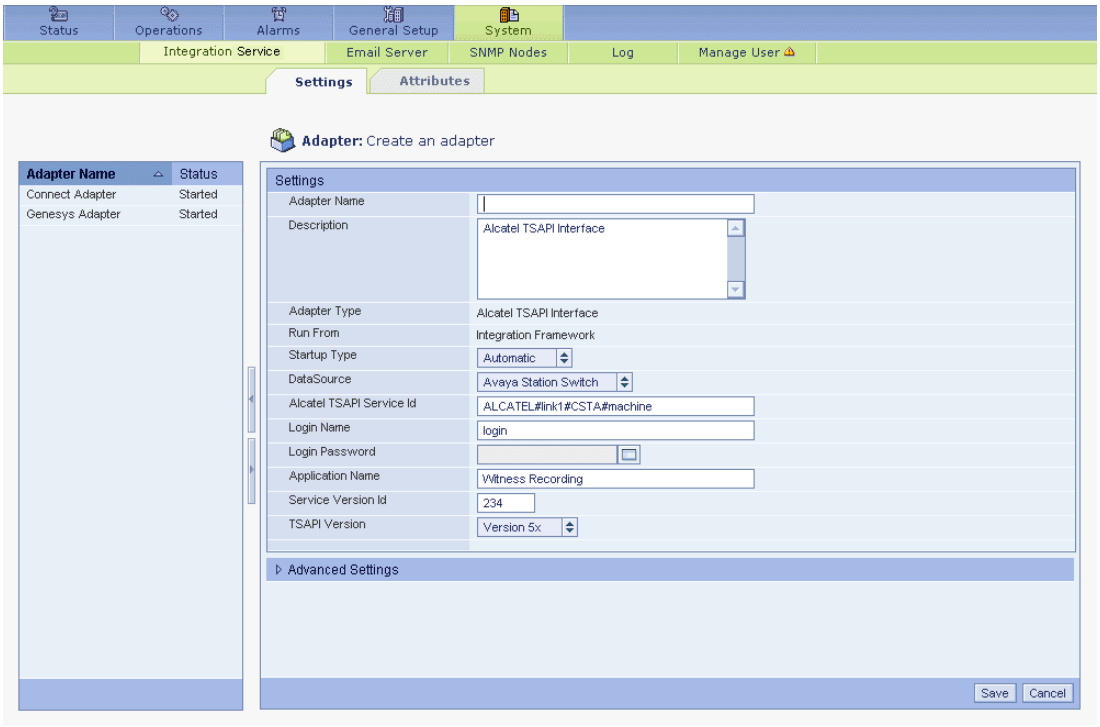
Use the following procedure to create a CTI adapter for the Alcatel Omni PCX 4400 switch using the Telephony Server Application Programming Interface (TSAPI).

To create an adapter for the Alcatel Omni PCX 4400 via TSAPI:

1 In the Recorder Manager, choose **System > Integration Service > Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **Alcatel TSAPI Interface**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.
Startup Type	Select a startup type: Automatic, Manual, or Disabled.
DataSource	Select a data source (see "Creating a Data Source" in the Integration Service Integration Guide).
Alcatel TSAPI Service Id	This is the internal identifier by which the switch is known to the Alcatel TSAPI Premium Server.
Login Name	Specify the login name used to access the TSAPI server (optional).
Login Password	Click the button beside the Password field to type a password used to access the TSAPI server (optional).
Service Version Id	This ID number identifies the type of voice recording system listening service. For Alcatel Version 5 or later switches (and some more recent version 4 switches), set to 234 (the default).

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Aspect Event Bridge

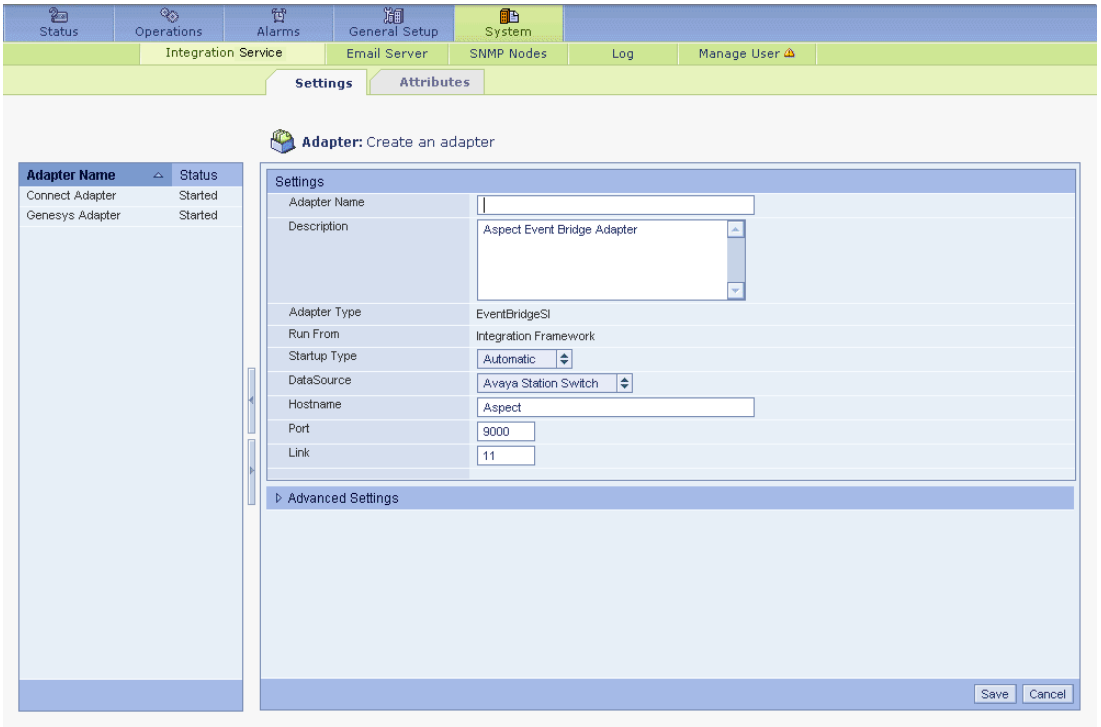
Use the following procedure to create a CTI adapter for an Aspect Event Bridge.

To create an Aspect Event Bridge Adapter:

1 In the Recorder Manager, choose **System > Integration Service > Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **Aspect Event Bridge Adapter**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
DataSource	Select a data source.
Hostname	Machine Name to which Event Bridge interface will attempt to connect on the Integration Service server. This name must match the name exactly as configured on the Data System Address on the Aspect switch, and is case-sensitive.
Port	Specify the port on which the CTI Adapter listens for connections from the Aspect Switch. The default is **9000**.
Link	Specify the Data Link Number on the Aspect Switch. The default is **11**.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Concerto for Aspect Unison/Ensemble/Ensemble Pro

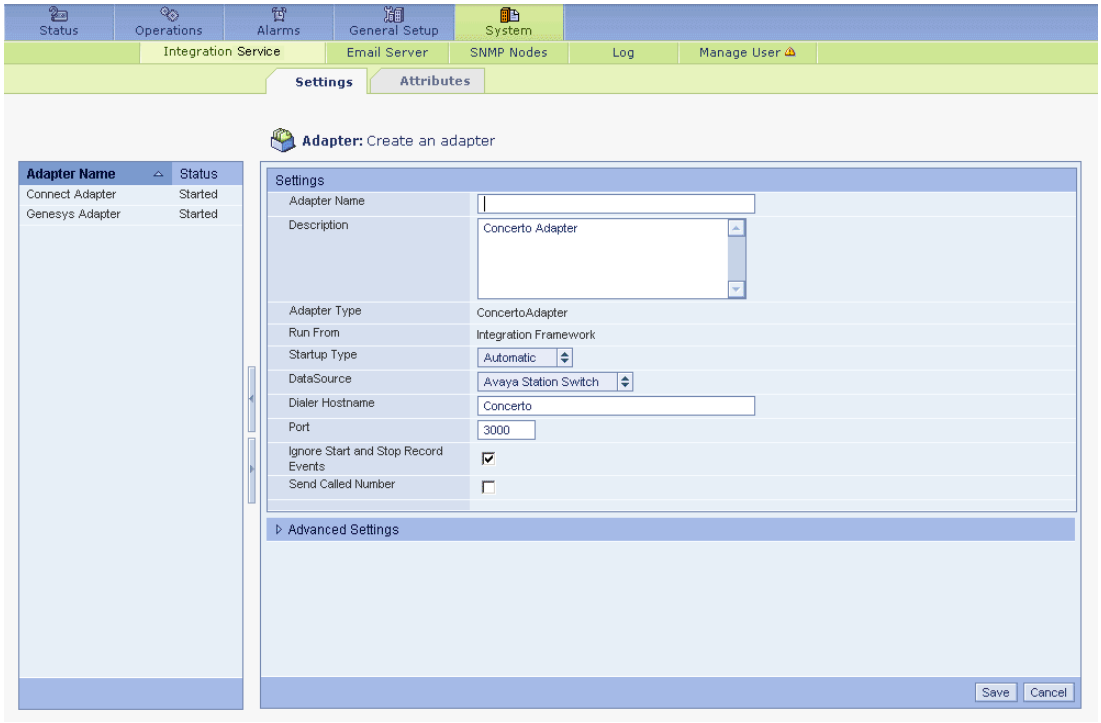
Use the following procedure to create a CTI adapter for an Aspect Unison/Ensemble/Ensemble Pro switch.

To create a Concerto adapter for Aspect Unison/Ensemble/Ensemble Pro:

1 In the Recorder Manager, choose **System** > **Integration Framework** > **Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **Concerto Adapter**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Data Source	Select a data source.
Dialer Hostname	Type the dialer host name. The default is **Concerto**.
Port	Specify the port on which the dialer listens for a connection from the CTI adapter. The default is **3000**.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Aspect Contact Server (Portal)

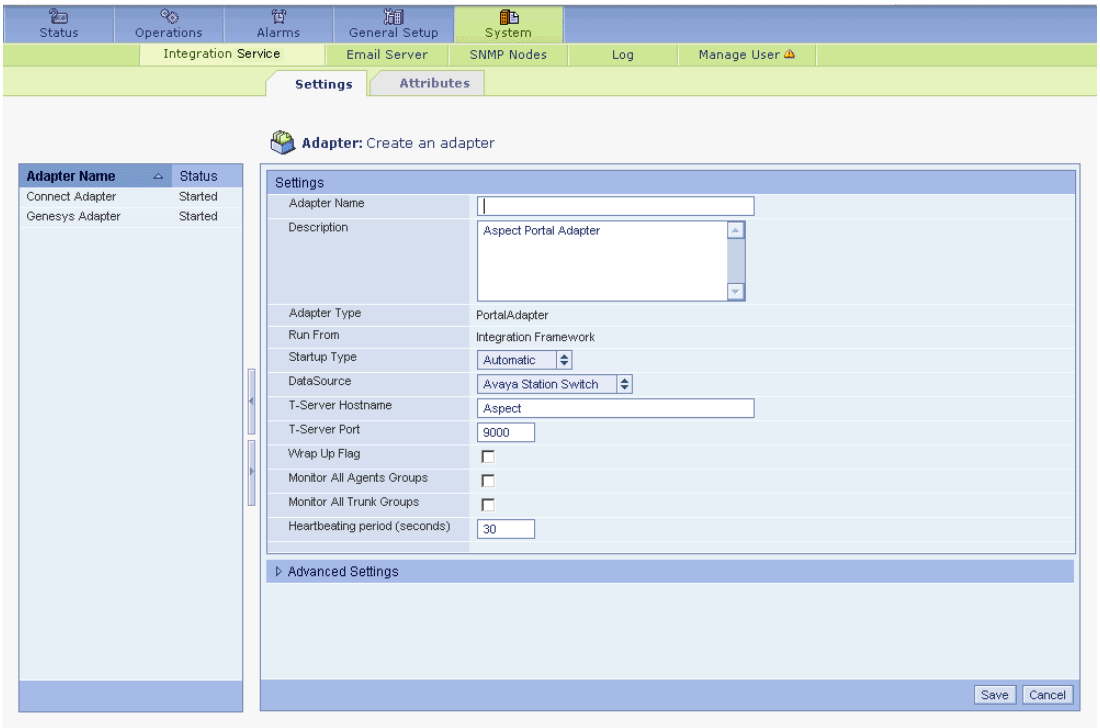
Use the following procedure to create a CTI adapter for an Aspect Contact Server (Portal).

To create an adapter for the Aspect Contact Server (portal):

1 In Recorder Manager, choose **System > Integration Service > Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **Aspect Portal Adapter**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.
T-Server Hostname	Type the a unique host name or IP address for the Aspect Contact Server (Portal) Server. The default is **Aspect**.
T-Server Port	The Aspect Contact Server (Portal) port number to which the CTI Adapter connects. The default is **9000**.
Wrap Up Flag	Select this check box if the CTI Adapter will receive all wrap-up events.
All Agent Groups	Select this check box if the CTI Adapter will receive CTI events for all Agent Groups (as defined on the Aspect switch).
All Trunk Groups	Select this check box if the CTI Adapter will register to receive CTI events for all Trunk Groups.
Heartbeating Period	Specify a number representing the number of seconds between requests. Set to **0** (zero) to disable. The default is **30**.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

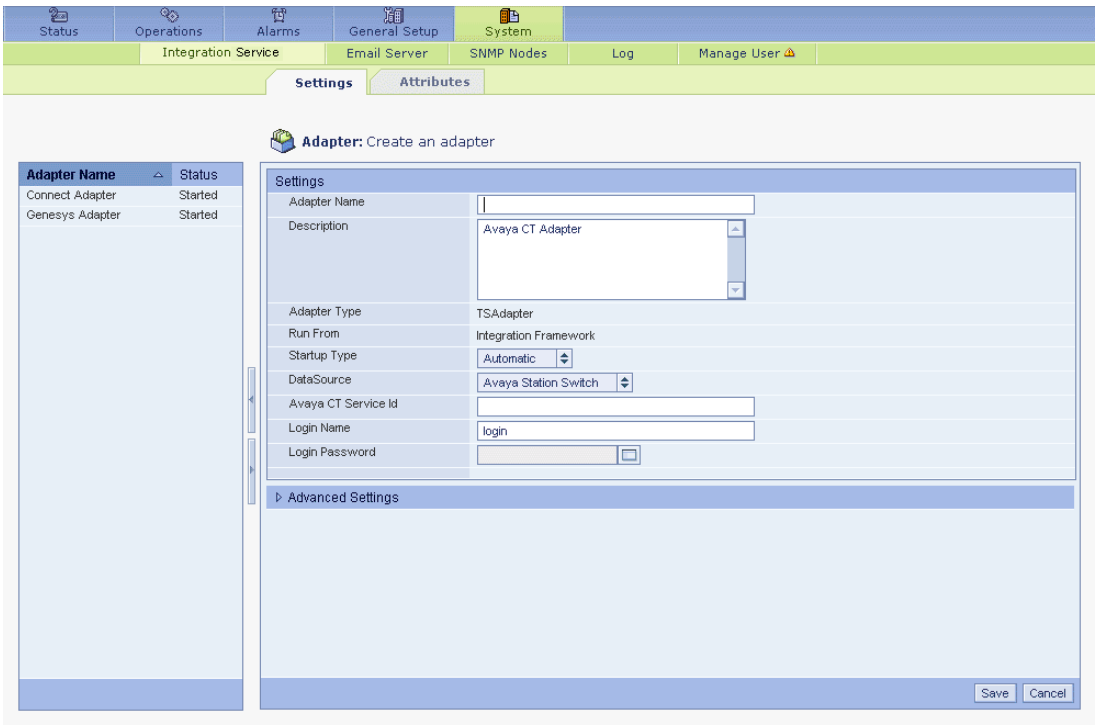
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Avaya Definity G3/S8x00 via TSAPI

Use the following procedure to create a CTI adapter for the Avaya Definity G3/S8x00 using the Avaya computer telephony (CT) server running the Telephony Server Application Programming Interface (TSAPI).

To create an adapter for the Avaya Definity G3/S8x00 via Avaya CT (TSAPI):

1. In the Recorder Manager, choose **System > Integration Service > Settings**.
2. Click **Create**.
3. In **Choose a CTI Adapter to Create**, select **Avaya CT Adapter**.



4. Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Adapter Type	This is a read-only field that specifies the adapter selected above.
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.
Avaya CT Service Id	This is the internal identifier by which the Avaya CT Server is known to the CTI Adapter's server.
Login Name	Type a login name used to access the TSAPI server (password).
Login Password	Click the button beside the **Password** field and type a password for the TSAPI server (optional).

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Avaya DLG Adapter

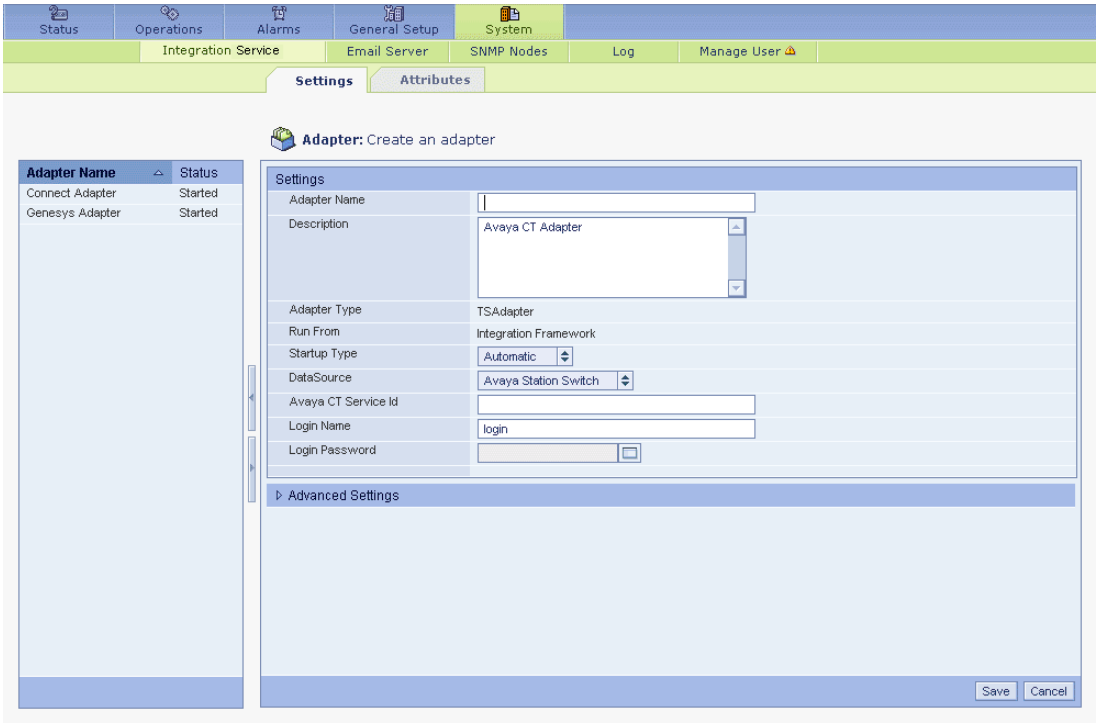
Use the following procedure to create a CTI adapter for the Avaya Definity G3/S8x00 switch using the Avaya Definity LAN Gateway (DLG) interface.

To create an Avaya DLG adapter:

1 In the Recorder Manager, choose **System > Integration Framework > Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **Avaya CT Adapter**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.
DLG hostname or address	Type the hostname or IP address of the AES server or MAPD card on which the DLG link resides.
Link Number	Type the number assigned to the DLG link.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

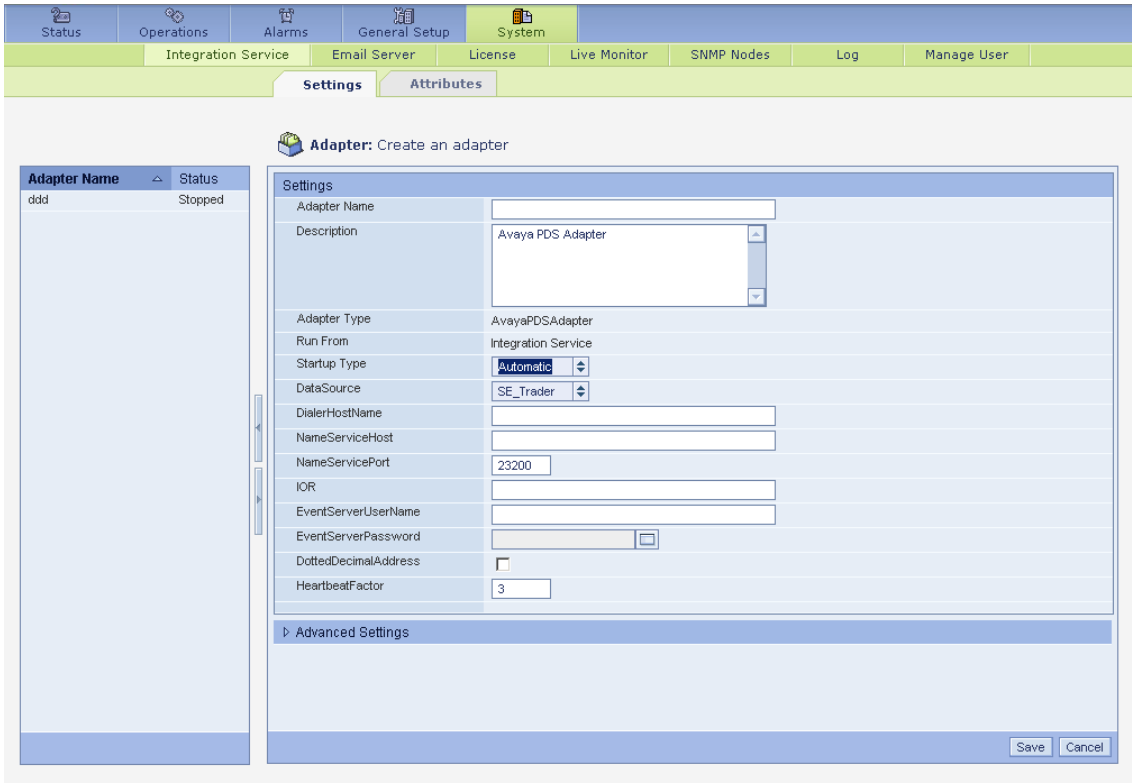
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Avaya PDS 12 and 3.0

Use the following procedure to create a CTI adapter for the Avaya predictive dialing system (PDS) for version 12 of the dialer using Administration Manager R3.0 (formerly Producer).

To create an Avaya PDS adapter for Avaya PDS 12 and 3.0:

1. In the Recorder Manager, choose **System > Integration Service > Settings**.
2. Click **Create**.
3. In **Choose a CTI Adapter to Create**, select **Avaya PDS Adapter**.



4. Specify settings for this adapter, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Adapter Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Adapter Type	This is a read-only field that specifies the adapter selected above.
Run From	This is a read-only field.
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source. This may be a ___, ___, or ___.
DialerHostName	Type the host name of the dialer.
NameServiceHost	Type the name or address of the name service host.
NameServicePort	Type the port number for the name service host specified above.
IOR	Type the name of the Interoperable Object Reference (IOR).
EventServerUserName	Type the user name for the event server.
EventServerPassword	Type the password for the event server.
DottedDecimalAddress	Type the dotted decimal address.
HeartbeatFactor	Enter a value for the heatbeat.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

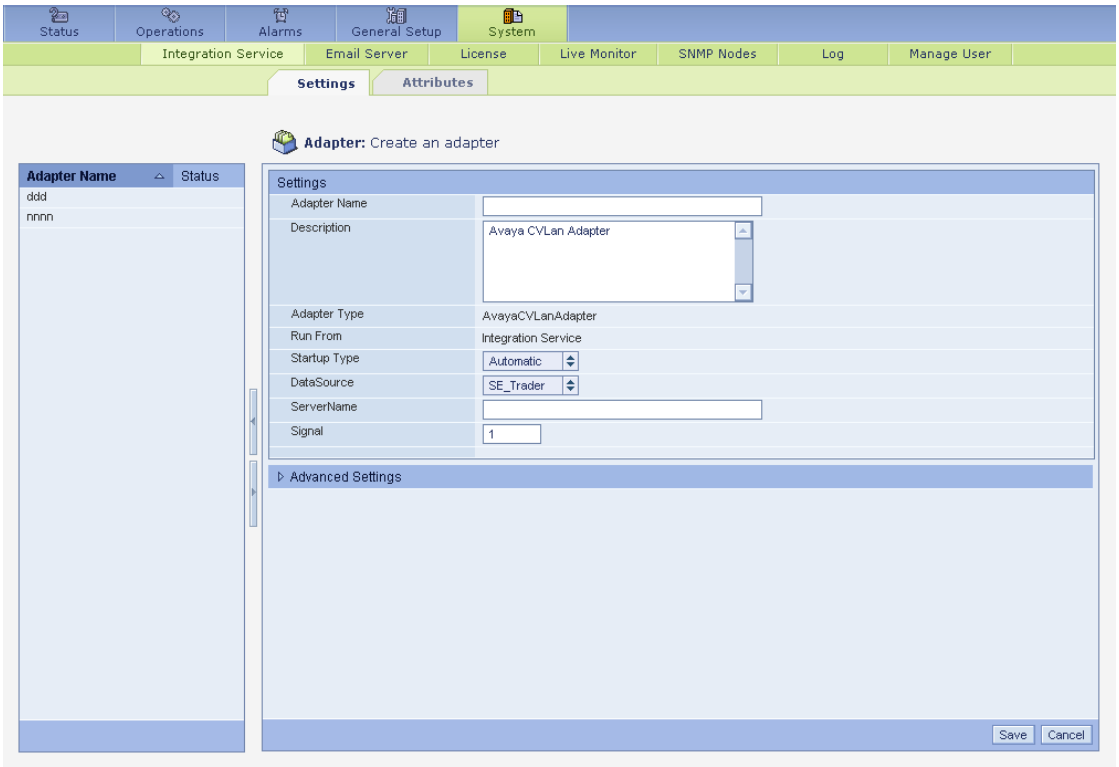
Avaya ASAI via CVLAN Adapter

Use the following procedure to create a CTI adapter for an Avaya switch using the Adjunct Switch Application Interface (ASAI) message set on CallVisor/LAN (CVLAN).

CVLAN is the original CTI API that allows programs to be written, using the ASAI message set, in the C: programming language.

To create a CVLAN adapter for Avaya ASAI:

1. In the Recorder Manager, choose **System > Integration Service > Settings**.
2. Click **Create**.
3. In **Choose a CTI Adapter to Create**, select **Avaya CVLAN Adapter**.



4. Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Adapter Type	This is a read-only field that specifies the adapter selected above.
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.
Hostname	Type the hostname or IP address of the AES server.
Signal	Type the number of the link to which you are connecting.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

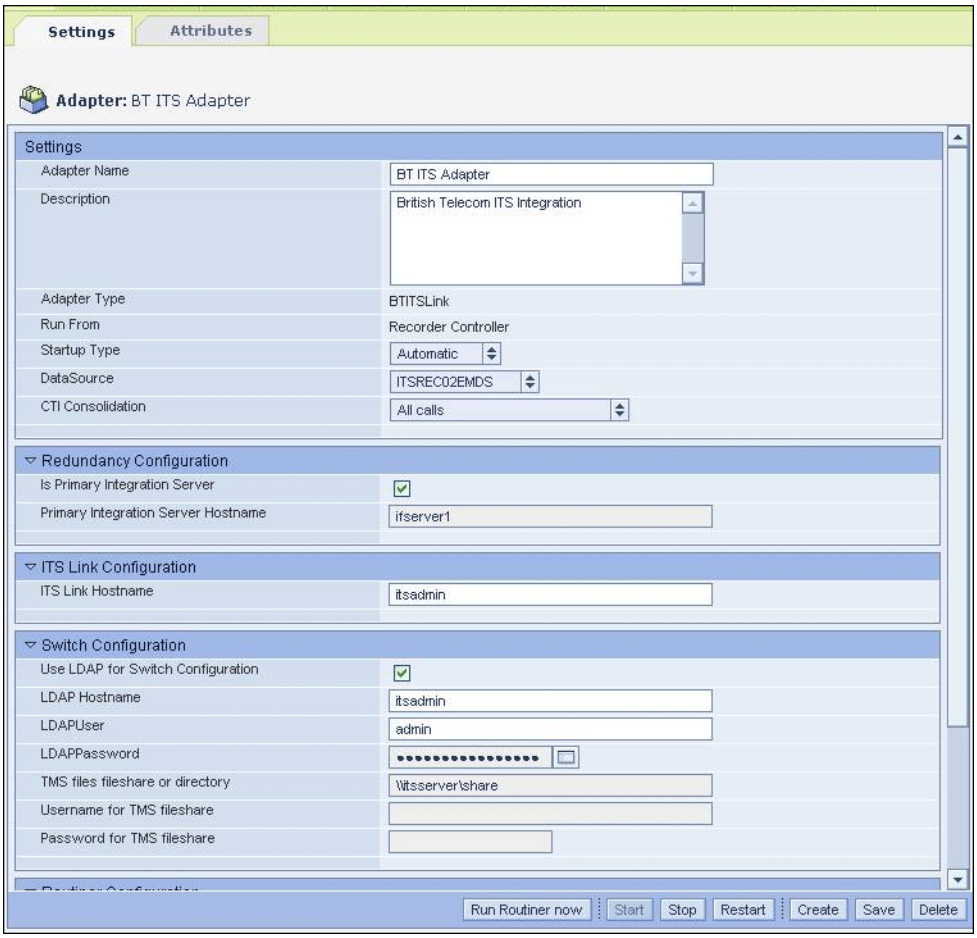
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

BT Integration

Use the following procedure to create a CTI Adapter for British Telecom Integration with the BT ITS switch.

To create an adapter for BT Integration:

1. In the Recorder Manager, choose **System > Integration Service > Settings**.
2. Click **Create**.
3. In **Choose a CTI Adapter to Create**, select **British Telecom ITS Integration**.



4. Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Settings	
Adapter Name	Type a unique name for this adapter (typically ITSLink). Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected.
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Type the Trader Data Source Name defined in Enterprise Manager.
CTI Consolidation	Select one of the following: • **All Calls** – CTI from ITS-Link recorded whether the call is recorded or not. • **CallsWithRecordedParty** – CTI from ITS-Link recorded if the recorded party is involved. • **OnlyRecordedParties** – CTI from ITS-Link recorded only for recorded parties.
Redundancy Configuration	
IS Primary Integration Server	Select the check box to make this the primary integration server (otherwise it will be the backup server).
Primary integration server hostname	Type the IP address or domain name of the server to use for failover purposes.
ITS Link Configuration	
ITS Link Hostname	Type the IP address or domain name for the ITS Link.
Switch Configuration	
Use LDAP for switch configuration	Select this check box to use the Lightweigt Directory Access Protocol (LDAP) for switch configuration (otherwise, the system uses .tms files). Once you check this, LDAP fields become required.
LDAP Hostname	Type the IP address or domain name for the LDAP host. This field is only configurable if you enable LDAP use by selecting the check box above. Required if the LDAP checkbox is enabled.
LDAP User	Type the username for accessing the LDAP database. Required if LDAP checkbox is enabled.
LDAP Password	Type the password for accessing the LDAP database. Required if LDAP checkbox is enabled.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
TMS files fileshare or directory	Type the path to the location of the TMS files. Typically these are located on the ITSLink server. This field is only configurable if you deselect the LDAP check box.
Username for TMS fileshare	Type the user name for the TMS fileshare. This field is only configurable if you deselect the LDAP check box.
Password for TMS fileshare	Type the password for the TMS fileshare. This field is only configurable if you deselect the LDAP check box.
Routiner Configuration	
Line for Routiner Use	Specify the line number for routiner use. This must be an unused PSTN line.
Steering Code	The steering code is sequence of digits that prefix those dialled by the Routiner. This enables the BT ITS Switch to improve performance by filtering Routiner calls away from the rest of the system. The prefix must not conflict with settings on the customer's PBX.
Schedule Routiner for daily checks	Select this check box to have the Routiner run daily checks (otherwise, you must run the Routiner manually by clicking the **Run Routiner Now** button.
Hour of day to run Routiner	Using 24-hour clock time, type an integer representing the hour of day on which you want Routiner to run. For example, to run at 2:00 am, you would enter **2**, or to run at 7:00 pm, you would enter **19**.This setting is only available if you enable daily routiner checks as described above.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

At any time, select the adapter and then click **Run Routiner Now** to run the Routiner.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

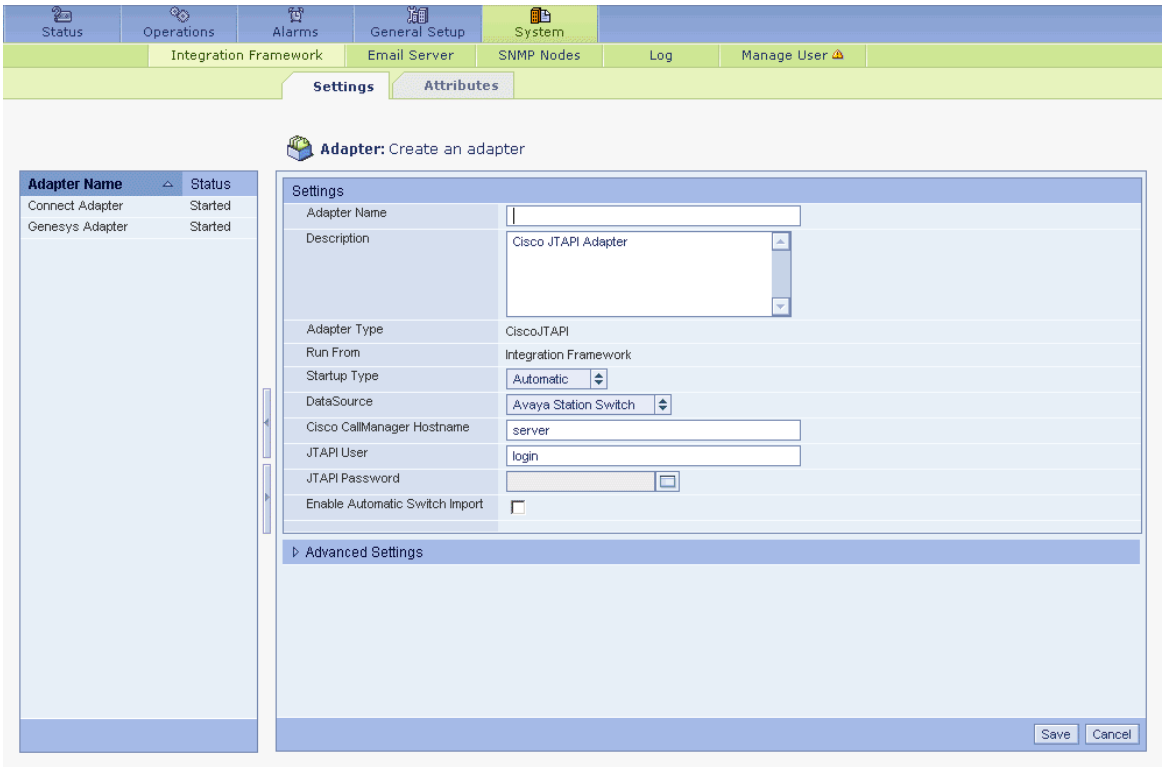
Cisco CallManager with JTAPI

Use the following procedure to create a CTI adapter for Avaya, Cisco Call Manager, or Cisco IP using the Java Telephony Application Programming Interface (JTAPI).

To create an adapter for the Cisco CallManager with JTAPI:

1 In Recorder Manager, choose **System > Integration Service > Settings**.

2 Click **Create,** and then select **Cisco JTAPI Adapter.**



3 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected in the previous step.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Run From	This is a read-only field that specifies the server from which the adapter is run.
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.
Cisco CallManager Host Name	Type the host name or IP address of the JTAPI sever.
JTAPI User	Type a login name used to access the JTAPI server
JTAPI Password	Click the Password button to enter a password used to access the JTAPI server.
Enable Automatic Switch Import	Select this check box to import switch information automatically.

4 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

5 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Cisco Call Manager

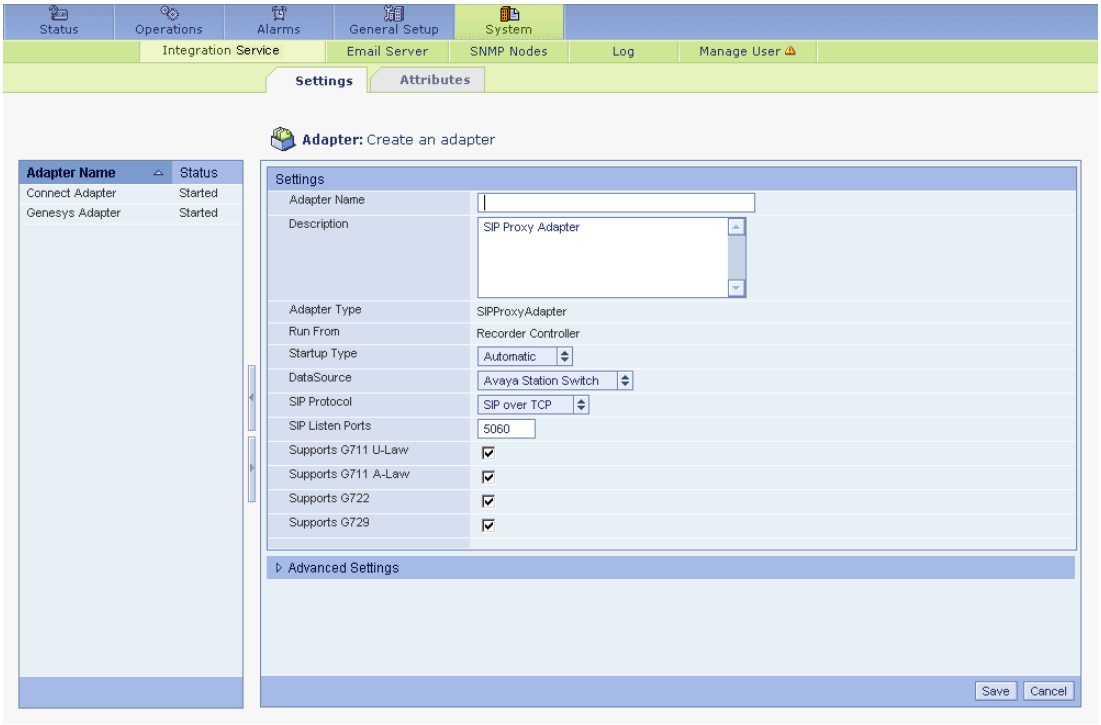
Use the following procedure to create a Cisco proxy adapter using session initiated protocol (SIP) for a Cisco CallManager that supports duplicate media streaming (DMS).

To create a Cisco SIP Proxy adapter to support Cisco DMS:

1 In the Recorder Manager, choose **System > Integration Service > Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **SIP Proxy Adapter.**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.
Protocol	Select the protocol (**UDP** or **TCP**) that the SIP Proxy adapter will use.
Ports	Specify the port(s) that the SIP Proxy Adapter will listen on, using commas to separate multiple port numbers.
Supports G711 U-Law	Select this check box if the adapter will advertise support of the G711 U-Law codec that the recording application will support.
Supports G711 A-Law	Select this check box is the adapter will advertise support of G711 A-Law codec that the recording application will support.
Supports G722	Select this check box if the adapter will advertise support of the G722 codec that the recording application will support.
Supports G729	Select this check box if the adapter will advertise support of the G729 codec that the recording application will support.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Genesys Adapter

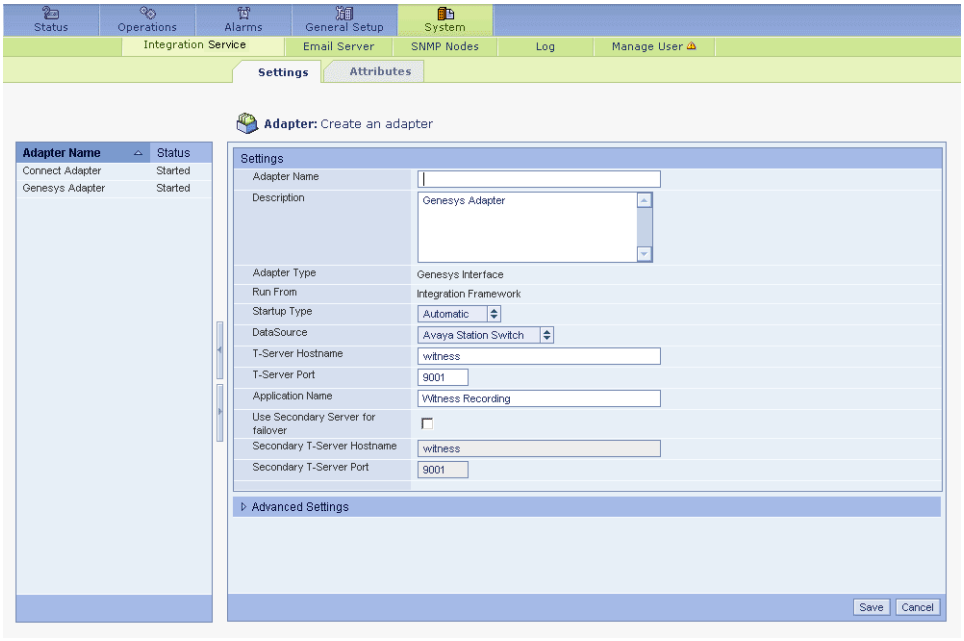
Use the following procedure to create a CTI adapter for a Genesys switch.

To create a Genesys adapter:

1 In the Recorder Manager, choose **System** > **Integration Service** > **Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **Genesys Adapter**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
T-Server Hostname	Type the name of the primary Genesys server (set to **witness** by default).
T-Server Port	Specify the port on which the primary TServer listens for connections from the clients. **9001** is the default.
Application Name	Identifies the key (section name) in the Genesys configuration file (tserver.cfg) that holds the configuration settings for the Genesys application from which the CTI Adapter obtains events. **Witness Recording** is the default.
Use Secondary Server for failover	Select this check box if you want to use a failover server.
Secondary T-Server Hostname	Type the name of the secondary Genesys server (set to **witness** by default). This field is required if you select the **Use Secondary Server for failover** check box.
Secondary T-Server Port	Specify the port on which the secondary TServer listens for connections from the clients. **9001** is the default. This field is required if you select the **Use Secondary Server for failover** check box.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

7 Select the adapter in the left-hand pane and click the **Start** button to start the adapter.

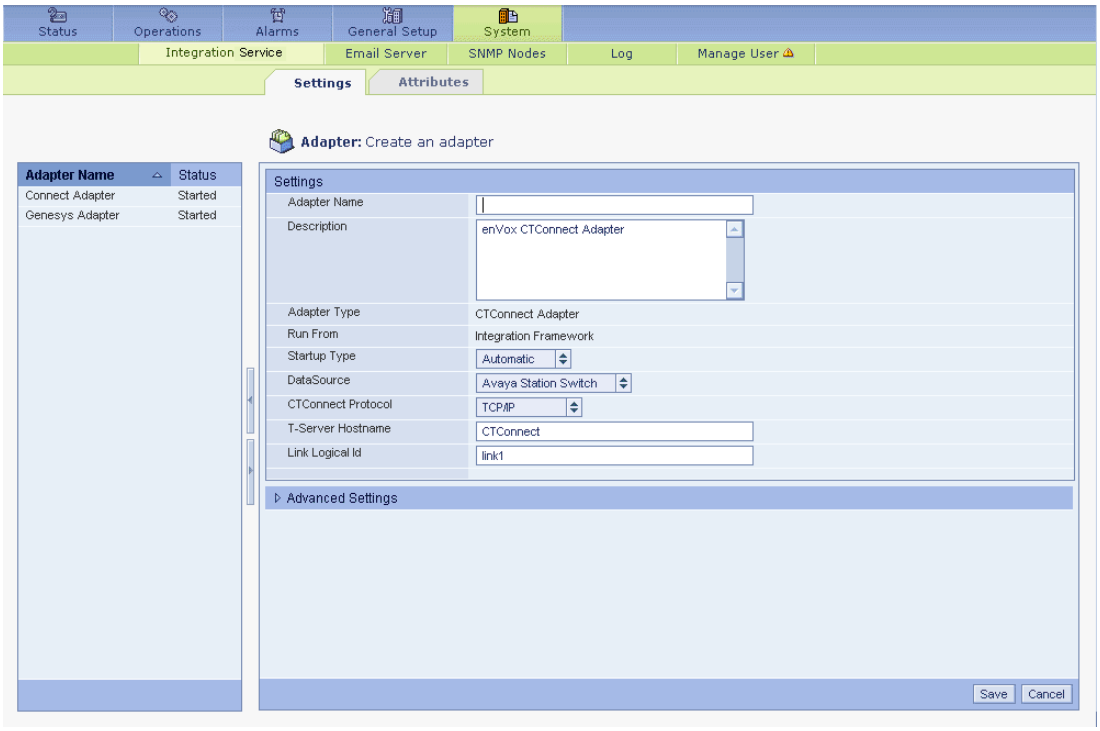
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Nortel Meridian/Succession via CTConnect

Use the following procedure to create an enVox CTConnect adapter for the Nortel Meridian/Succession switch.

To create an enVox CTConnect adapter:

1. In the Recorder Manager, choose **System > Integration Service > Settings**.
2. Click **Create**.
3. In **Choose a CTI Adapter to Create**, select **enVox CTConnect Adapter**.



4. Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.
CTConnect Protocol	Defines the type of connection used to connect to the CTI Adapter host. The network type is closely related to and must be consistent with the IP address provided. Select one of the following: • **ncacn_ip_tcp** for TCP/IP • **ncalrpc** for Local RPC • **ncacn_np** for named Pipes • **ncadg_ip_udp** for UDP/IP
T-Server Hostname	Type the network name of the CTConnect server. This field is set to **CTConnect** by default.
Link Logical Id	The logical identifier for the switch. The identifier must match the **Logical Identifier** for the **Switch Link**, as configured on the Intel NetMerge CPS (CT Connect) server. Refer to your Intel NetMerge CPS (CT Connect) documentation for more information about these fields. This field is set to **link1** by default.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Nortel Meridian/Succession via MLS

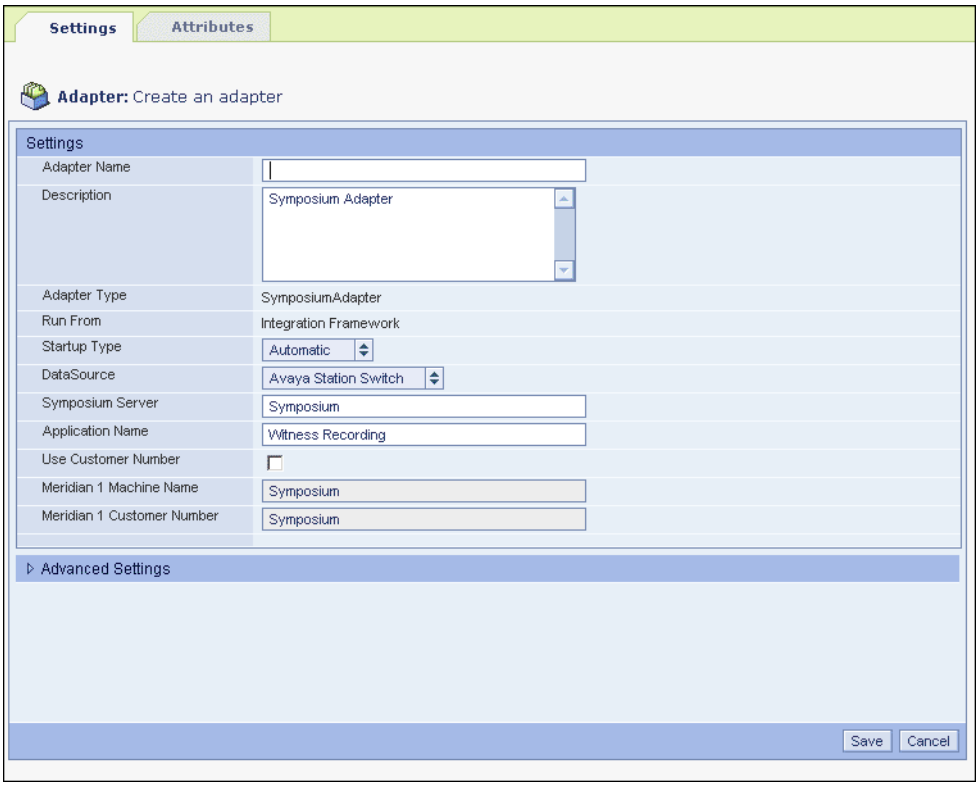
Use the following procedure to create a CTI Adapter for a Symposium server for the Nortel Meridian/Succession switch using Meridian Link Services (MLS).

To create a Symposium adapter for Nortel Meridian/Succession:

1 In the Recorder Manager, choose **System > Integration Service > Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **Symposium Adapter**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.
Symposium Server	The host name or IP address of the Symposium server.
Application Name	This is a required field.
Use Customer Number	Check this box if you want to use a customer number.
Meridian1Machine Name	Required if you select the **UseCustomerNumber** check box. This is the Machine ID from the Contact Centre Server (defaults to SL16).
Meridian1Customer Number	Required if you select the **UseCustomerNumber** check box. This is the Switch Customer Number from the Contact Center Server Information Screen.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

ICM Adapter

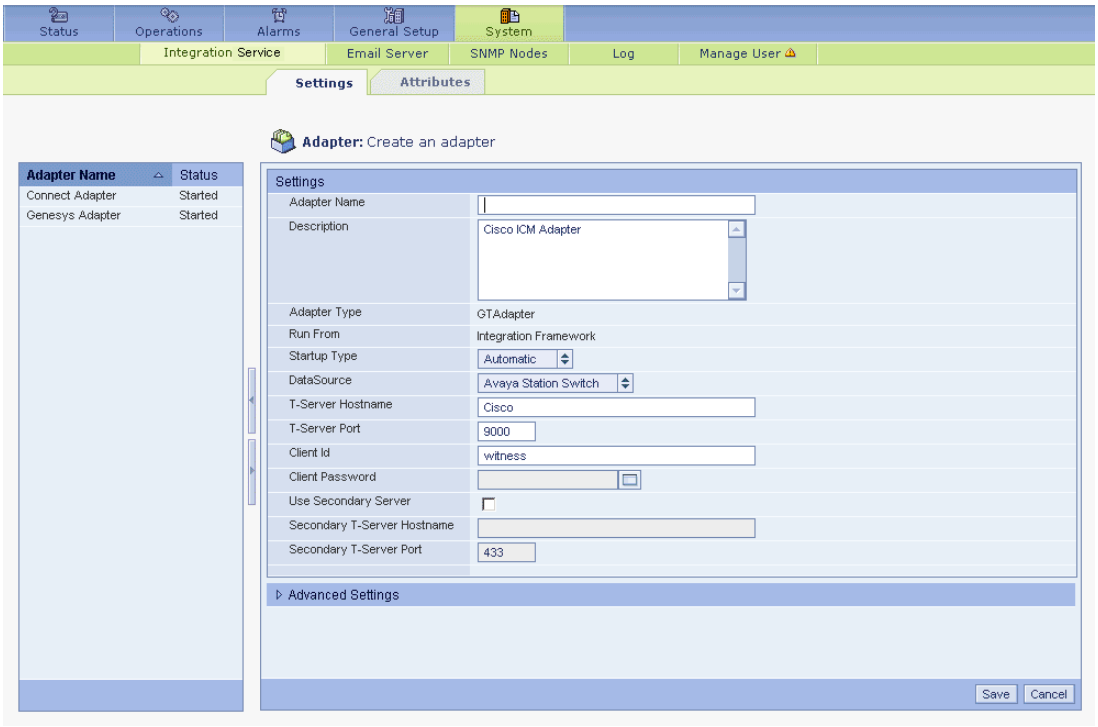
Use this procedure to create a Cisco Intelligent Contact Management (ICM) adapter for use with Avaya, Cisco Call Manager, or Cisco IP.

To create an ICM adapter:

1 In the Recorder Manager, choose **System > Integration Service > Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **Cisco ICM Adapter**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.
DataSource	Select a data source.
T-Server Hostname	Type the Host name or IP address of the primary Cisco ICM (GeoTel) server. **Cisco** is the default.
T-Server Port	Specify the connection port on the primary Cisco ICM (GeoTel) server. **9000** is the default.
Client ID	Type a login name used to access the Cisco ICM (GeoTel) server (set to **witness** by default).
Client Password	Click the button beside the ClientPassword to type a Password used to access the Cisco ICM (GeoTel) server.
Use Secondary Server	Select this check box if you want to use a failover server.
Secondary T-Server Hostname	Specify the host name or IP address of the backup Cisco ICM (GeoTel) server. This field is required if you select the **UseFailoverServer** check box.
Secondary T-Server Port	Specify the connection port on the backup Cisco ICM (GeoTel) server. **433** is the default. This field is required if you select the **UseFailoverServer** check box.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

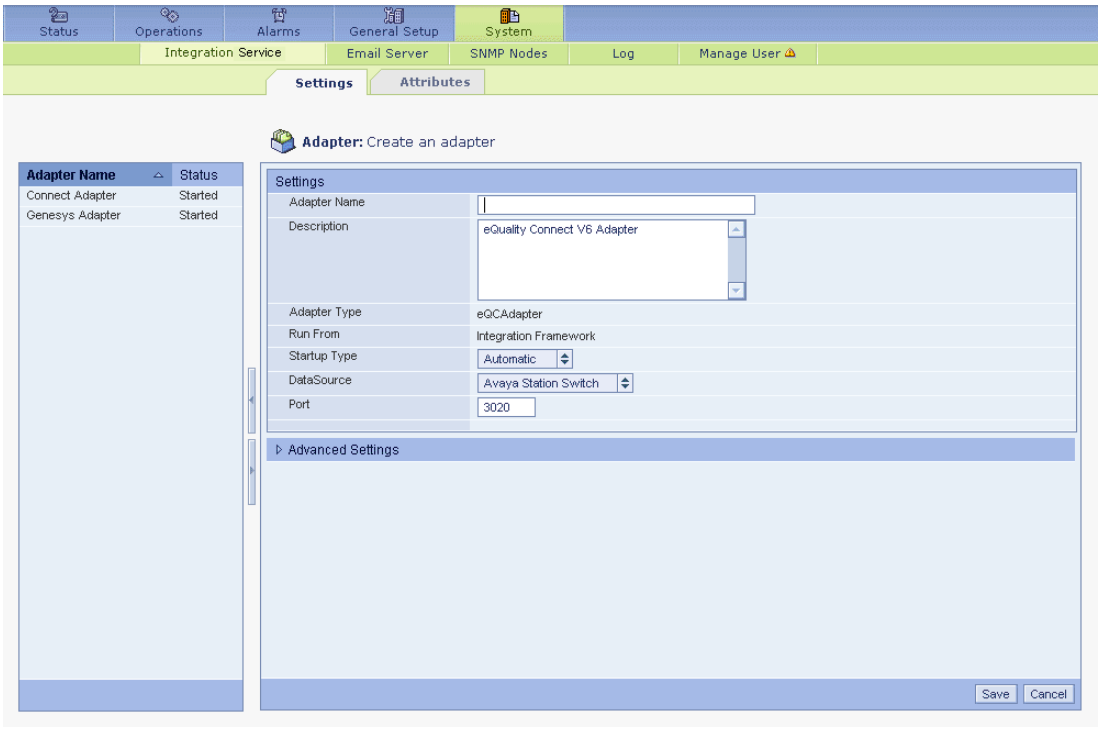
© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

eQuality Connect

Use the following procedure to create a CTI Adapter for eQuality Connect Integrations, including agent initiated monitoring (AIM) functionality or other custom integrations (such as email and web chat integrations, neither of which are currently supported).

To create an eQuality Connect adapter:

1. In Recorder Manager, choose **System > Integration Service > Settings**.
2. Click **Create**.
3. In the right-hand pane, in **Choose a CTI Adapter to Create**, select **eQuality Connect v6 Adapter**.



4. Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected above.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
Startup Type	Select a startup type: **Automatic, Manual,** or **Disabled**.
DataSource	Select a data source — this should be the switch used in Quality Monitoring. For more information refer to the section **Creating a Data Source** in the Integration Service Integration Guide.
Port	Specify the port number on which the eQCAdapter listens for connections. The default is 3020.

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Exec Record and TCP/IP API/Unify

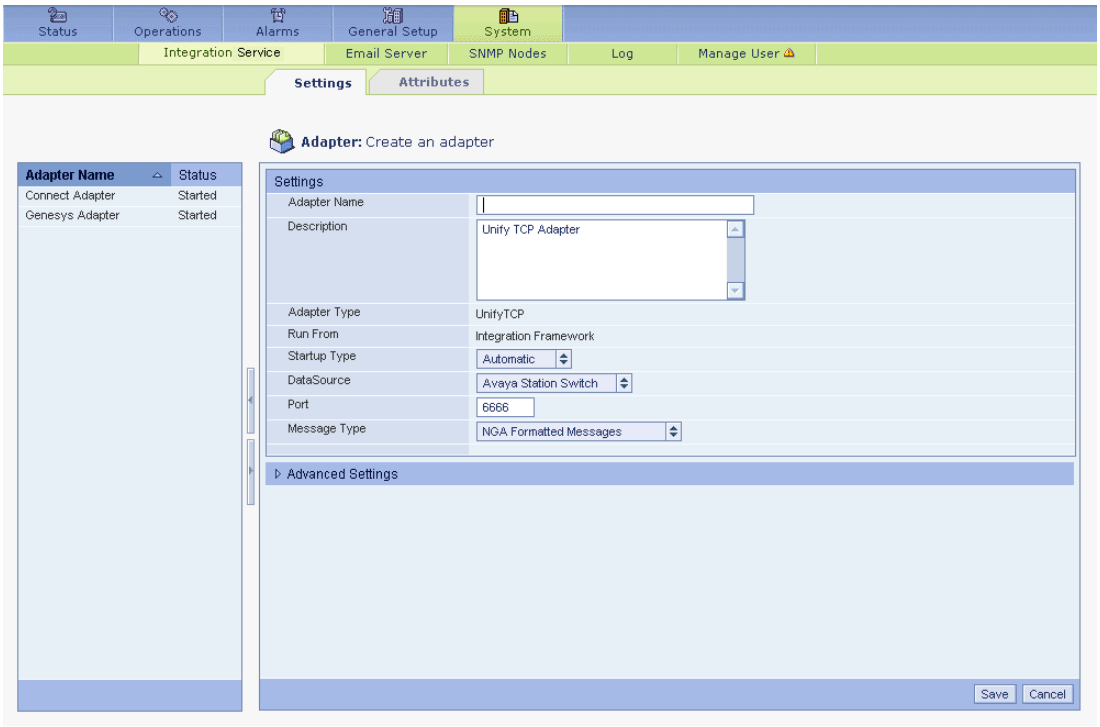
Use the following procedure to create a CTI Adapter for Exec Record and the TCP/IP API or Unify's transmission control protocol (TCP).

To create an adapter for Exec Record and TCP/IP API using Unify TCP:

1 In the Recorder Manager, choose **System > Integration Framework > Settings**.

2 Click **Create**.

3 In **Choose a CTI Adapter to Create**, select **Unify TCP Adapter**.



4 Specify settings for this adapter in the right-hand pane, referring to the following table (all fields are required unless otherwise indicated):

Field	Description
Name	Type a unique name for this adapter. Do not use any special characters or characters that truncate xml. This field is not case sensitive.
Description	Type a description of the adapter (optional).
Adapter Type	This is a read-only field that specifies the adapter selected.
Startup Type	Select a startup type: **Automatic**, **Manual**, or **Disabled**.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Field	Description
DataSource	Select a data source.
Port	Specify the port that the Unify TCP adapter is listening on. The default is **6666**.
Message Type	Select the MessageType.NGAType option if you will use the adapter for ExecRecord functionality. Select MessageType.DesktopApplMsg if you will use the adapter for recording control

5 Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.

6 Click **Save**. The adapter appears in the left-hand pane.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Glossary

Term	Definition
ACD	Abbreviation for Automatic Call Distribution. A system used to distribute calls placed to a call center to Agents when they are free. The system manages customer queues to make this process as efficient as possible. Unlike a PBX, there are more inbound telephone lines than Agents. The switch is typically non-blocking in that any call can be routed to any agent.
Agent	Any person who receives or makes contact with customers or prospects on behalf of an organization in a customer interaction center environment. Agents receive contacts via telephone, e-mail, and web interactions with customers, and are usually the first point of contact with customers.
Business Rule	A simple or complex logical statement, which determines the action to occur when a set of defined attributes and conditions are met for a customer interaction to become a Contact. Contacts are used to play back, annotate, and evaluate agent performance to achieve business goals and professional development. Business rules can be as simple as recording contacts, which occur on scheduled days of the week, or when a specific event happens. They can be as complex as including many AND/OR statements in a logical structure.
Capture Engine	A software component in all Recorders forming part of the Recorder subsystem. that interfaces with the TDM telephony infrastructure or IP Telephony network infrastructure to capture and record the audio/video contents plus associated or non-associated metadata of a customer Contact. A Capture Engine can be either a TDM type (eRecorder) or an IP type (IPCapture).
Data Source	A term for any source of recordable data or agent state information that an integration in the Integration Service will plug into, such as a customer's switch, capture system, or e-mail/e-mail integration system.

DNIS	Dialed Number Identification Service. A feature of 800 and 900 lines that provide the number that the caller dialed to reach the attached telephony system. The switch uses the DNIS to route calls to the appropriate agent or groups of agents.
DTMF	Dual Tone Multi Frequency, the mechanism of using dual tones to identify the keys pressed on a telephone set.
DTMFDigits	A call data attribute that indicates the MTMF digits that were pressed during the call. These digits could have been pressed by either party. This attribute is often used when the line itself does not encode called party information, so that the DTMF digits are use to determine who the agent was calling.
Enterprise Manager	A software enterprise management tool that allows you to control all aspects of recording and workforce optimization within an organization, such as adding workers and setting up sites and recorders. The Enterprise Manager is connected to, and can control, all recorders within the enterprise by interfacing with each Recorder Manager.
Extension	The telephone extension or line used by the party to be recorded or monitored.
Full time recording	Telephony term for recording the majority of contacts rather than "selective" recording. "Full time" replaces the term compliance recording as many users wish to record all of their contacts even though there is no legal requirement. The term also replaces "100%" recording in that in reality even in a large-scale recording system there are extensions that are not to be recorded or only parts of calls that are to be recorded due to security or business requirements. In addition, in Full-time Recording the recorder monitors a fixed set of lines as defined by its configuration. The delivery of Full-time Recording is primarily through passive tap techniques because it does not require expensive switch resources as the number of recording channels increases.
HTTPS (also S-HTTP)	Abbreviation for secure Hypertext Transfer Protocol. This is the same protocol as HTTP except it is encrypted to allow security, requiring a digital key to encrypt and decrypt HTTPS packets. Usually used with the Secure Socket Layer (SSL) enabling of web servers.
Integration Service	A system of hardware and software devices that integrates third-party data sources (such as switches) and drives in the recording subsystem with content and state information.
IP Analyzer	An optional hardware component used in some IP recording environments to analyze call control messages on the attached network and forward recording control messages to remote recorders.
IP Recording	A type of contact recording system where the capture engine detects (that is, sniffs) voice signals in a data network using the Internet Protocol of packets of information in a virtual envelope (VoIP), as opposed to TDM channel recording.
Live Monitoring	An application that enables users with authority based on their roles to observe both sides of the agent-customer interaction. Users can see and hear a contact in real time, while the interaction is actually taking place.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Local Archiver	A software component in all Recorders that archives a Contact's audio and video content plus associated metadata to a removable storage media, such as a DVD or tape. Local Archiver is part of the Recording Subsystem.
Observer	A thick-client Visual Basic application, related to the thin client Web Observer application, used to live monitor Contact(s).
Passive Tap Recording	A CTI method of recording the voice portion of a contact from the incoming trunk (T1 line) between public switching and the PBX. This process is implemented by placing a junction box on the inbound T1s. There must be one junction box per T1 to be used for trunk-side recording. For example, to monitor five trunks, five junction boxes are needed.
Passive Tap Station-Side Recording	A CTI method of recording contacts between the switch and a phone by tapping into the line that connects the switch to the telephone punch-down block, using a Y-cable so that each extension connects directly to a port on the voice card.
Passive Tap Trunk-Side Recording	A CTI method of recording voice data directly from an incoming trunk (T1 or E1 line) between public switching and a PBX or between two PBXs, allowing the recording of every call that comes into the PBX.
PBX	See Private Branch Exchange.
PCM32	Abbreviation for Pulse Code Modulation 32. PCM32 is a transmission system with a 2048 KB/s rate. All 32 channels are available for voice transmission. In the voice recording market, this is primarily used by trading systems as a link from their switch to the voice recorder.
Private Branch Exchange (PBX)	A PBX is a telephone switch owned privately, usually by a large company. If it owns a PBX, a company does not need to lease a telephone line for each telephone set at a site
Punch-Down Block	A wiring device used in telecom environments to connect wires between the switch and the telephone. It creates a junction point for connecting additional devices to the same set of wires without disconnecting the phone.
Recorder Manager	The software management tool installed locally on every Recorder that allows you to control all aspects of the Recorder, such as setting up media devices and managing voice cards. Each Recorder Manager within an organization connects to, and can be controlled by, the Enterprise Manager.
Retriever/Content Server	A software component in all Recorders that retrieves recorded content from the Recorder's storage media, such as hard drives, DVD disks, or tapes, after an HTTP-based request from applications has been made.
SCCP	Abbreviation for Cisco's Skinny Call Control Protocol, which is a proprietary protocol used between Cisco Call Manager and Cisco VoIP phones that defines a simple and easy-to-use architecture for transporting data packets by using the phone as the thin (i.e. skinny) client over IP in the context of H.323.

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Screen recording	The term used for the capture of a graphical representation of what was displayed on the Agent's PC or other terminal screen within the Call Center. When the screen recording is replayed by the Supervisor, the screen activity is played like a movie of the screen. Not all data is captured in order to reduce the bandwidth of the recording. Various schemes are used to capture only those areas of change.
SIP	Session Initiated Protocol. SIP is a standard, multi-media protocol for setting up, modifying, and terminating VoIP connections that operates at the application layer to negotiate reliable VoIP channels.
Station-side	Term used to indicate passive tapping of the user phone lines or extensions, rather than the incoming phone lines from the Public Switched Telephone Network (PSTN) to the PBX or ACD.
Station-side Recording	In passive tap-station-side recording, information is recorded between the switch and an extension itself. This is done by tapping into the line leaving the switch (PBX) to the telephone punch-down block (as opposed to trunk-side recording, which taps lines coming from the PSTN).
TDM	Abbreviation for Time-Division Multiplexing. In TDM, data streams are assigned different time slots on a single channel, which distinguishes TDM from other types of multiplexing.
Trunk	A single circuit or channel from a PBX to a carrier (for example, a T1 has 24 trunks). As a business rule attribute, this name identifies the specific circuit or channel being used in an external call.
Trunk Span	A group of related trunks that all form the same connection. Unlike a single trunk, a trunk span can conduct multiple exchanges of data simultaneously. A trunk span is used when high bandwidth is required.
Trunkside Recording	A method of recording information from the incoming trunk (T1 line) between public switching and the PBX.
VoIP	Voice Over Internet Protocol. This is a technology used to transmit voice conversations over a data network using the Internet Protocol of data packets of information in a virtual envelope.
VOX	Voice Operated Transmitter. This term refers to the method by which the Recorder detects that a call has begun (that is, tap-sense). The VOX method "listens" for voice on the line rather than using signaling information.
Web Observer	Web based thin-client application, related to the Observer thick client application, used to live monitor contact(s).

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Index

A

about this guide 7
acknowledging alarms 192
active alarms 191
activity auditing 238
adapter
  Alcatel 4400 via TSAPI 263
  Aspect Contact Server (Portal) 269
  Aspect Event Bridge 265
  Aspect Unison/Ensemble 267
  Avaya ASAI via CVLAN 277
  Avaya Definity/S8x00 via TSAPI 271
  Avaya DLG adapter 273
  Avaya PDS 12 and 3.0 275
  BT Integration 279
  Cisco Call Manager with JTAPI 282
  Cisco IP Call Manager 284
  CTI 38
  custom attributes 42
  eQuality Connect 294
  Exec Record and TCP/IP API/Unify 296
  Genesys 286
  ICM for Avaya 292
  ICM for Cisco Call Manager 292
  Nortel Meridian/Succession via CTConnect 288
  Nortel Meridian/Succession via MLS 290
  selecting 39
  settings 38, 41
  starting and stopping 42
add extensions 225
adding users 28
additional resources 15
agents, managing 224
Ai-Logix, compatible voice cards 242
alarms
  acknowledging 192
  alarm priority level 188
  analyzer 174
  audible notication 189
  configuring 185
  delete notification profile 199
  editing 187
  history, clearing 193
  monitoring and viewing 191
  monitoring components 184
  notification profiles 196
  priority 185, 187, 191
  profiles, assigining 188
  schedules 188
  silence 191
  SNMP 202
  summary 244
  viewing active 191
  viewing and monioring 191
  viewing settings 185
Alcatel 4400 via TSAPI 263
analog voice cards
  channel identifiers 152
  channels 150
  modifying 149
Analyzer 166
analyzer
  accessing 171
  alarms 174
  component logs 174
  configuring call control 177

create call control group . . . 179
edit call control group . . . 180
e-mail . . . 176
export and import . . . 175
import and export . . . 175
IP addresses . . . 175
logs . . . 176
managing users . . . 176
network settings . . . 175
preferences . . . 176
recorder groups, add . . . 175
settings . . . 175
start and stop . . . 174
status . . . 171
analyzer protocol . . . 165
application controlled, extension recording mode . . . 90
archive
centralized, configuring . . . 108
configuring media to be managed . . . 218
failover . . . 74
local media tasks . . . 66
replacing a physical device . . . 74
archive device, adding . . . 214
attributes
editing . . . 101
live monitor . . . 101
live monitor, create . . . 101
live monitor, managing . . . 102
tags, adding and deleting . . . 103
audible notification, alarms . . . 189
audio compression . . . 84
audit logs
recorder manager . . . 238
trace logs . . . 238
Viewer . . . 238
Windows Event Viewer . . . 239
auditing . . . 238
authorized users . . . 27
Avaya Definity/S8x00 via TSAPI . . . 271
Avaya h.323 . . . 166

B

backup and restore . . . 226

C

CAL . . . 79
call buffer . . . 62
call buffer, change location . . . 64
call control
analyzer . . . 175
configuring . . . 177
edit group . . . 180
recording group . . . 179
viewing settings . . . 177
CAM - See Archive . . . 108
capture status . . . 52
cards and filters . . . 159
centralized archiving . . . 108
Centralized Archiving failover . . . 74
channel identifiers
analog . . . 152
Cybertech . . . 148
NGX voice cards . . . 141
PCM32 voice cards . . . 134
channels
analog, modifying . . . 150
channel assignment tutorial . . . 155
configuring . . . 118
Cybertech, updating . . . 146
editing tags . . . 119
estimating for live monitor . . . 95
NGX, updating . . . 139
PCM32 . . . 132
screen recording . . . 62, 106
T1/E1 . . . 125
voice card . . . 117
checksum, correcting . . . 259
CIC . . . 16
Cisco Call Manager with JTAPI . . . 282
Cisco Call Manager, active recording . . . 166
Cisco IP Call Manager . . . 284
clearing alarm history . . . 193
clearing component logs . . . 211
cloning recorders . . . 227
codecs . . . 84
column mapping, observer . . . 97
columns, re-arranging . . . 104
command line
correcting tampering . . . 261
compatible voice cards, Ai-Logix . . . 242
component logs, clearing . . . 174, 211
component logs, exporting . . . 208
components
compressor . . . 84
configuring common . . . 46
consolidator . . . 79
disk manager . . . 77
monitoring with alarms . . . 184
start and stop . . . 59
voice cards . . . 111
composite query template, remote archive . . . 108
compression . . . 84
consolidator
configuring . . . 79

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

creating database server 80
database server, deleting 82
database server, edit 82
database settings 79
contacts, pruning 225
conventions used in this guide 13
CTI adapter
Alcatel 4400 via TSAPI 263
Aspect Contact Server 269
Aspect Event Bridge 265
Aspect Unison/Ensemble/Ensemble Pro 267
Avaya ASAI via CVLAN 277
Avaya Definity/S8x00 via TSAPI 271
Avaya DLG Adapter 273
Avaya PDS 12 and 3.0 275
BT Integration 279
Cisco Call Manager with JTAPI 282
Cisco IP Call Manager 284
configuring 38
eQuality Connect 294
Exec Record and TCP/IP API/Unify 296
Genesys 286
ICM for Avaya 292
ICM for Cisco Call Manager 292
ICM for Cisco IP 292
Nortel Meridian/Succession via CTConnect 288
Nortel Meridian/Succession via MLS 290
CTI Studio 225
custom attributes 42
Customer Access License 79
Customer Interaction Center 16
Cybertech voice cards
channel identifiers 148
channels, updating 146
modifying 142
update personality 148

D

data channels used for tagging only diagnostics tool . . 257
database server, consolidator 80
database settings, consolidator 79
defining the live monitor server 95
defragment hard drives 223
diagnostics tools 257
disk management 222
disk manager
configuring 77
drives,viewing 78
settings 77
system maintenance 222
do not record, recording mode 86
duplicating recorders 227

E

e-mail
adding analyzer email server 176
adding server settings 200
configuring servers 200
testing settings 201
end users, creating 27
Ensemble, CTI adapter 267
eQuality Connect adapter 294
event viewer in Windows 239
Exec Record and TCP/IP API/Unify adapter 296
Exec Recorder adapter 296
ExecRecord 86, 91
existing 106
exporting component logs 208
exporting configuration information 206
extensions
adding (TDM) 224
advanced recording mode 86
creating 88
deleting 91
editing 90
finding 88
managing 86
E1, modifying protocol 128

F

failover, archive 74
filters and cards 159
finger printing 63, 259
framer errors 234
Funk screen recording 105

G

G711 84
G722 84
G.726 84

H

hard drive, replacing 216
help, online 35
history, alarm 193
HP SIM, configure SNMP 204

I

ICM for Avaya 292
ICM for Cisco Call Manager 292
ICM for Cisco IP 292
identifying a voice card 113
importing configuration information 207

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

Integration Service
CTI adapter . . . 38
screen recording . . . 106
status summary . . . 54
intended audience . . . 8

L

LDAP . . . 280
license . . . 105
activating . . . 23
configuring . . . 23
reactivating . . . 23
Lightweigt Directory Access Protocol (LDAP) . . . 280
Live Monitor
extension recording mode . . . 91
live monitor . . . 101
configuring Observer . . . 98
create columns . . . 101
managing attributes . . . 102
observer column mapping . . . 97
observer column order . . . 104
replay restrictions . . . 104
server, defining . . . 95
sizing for . . . 95
troubleshooting . . . 105
local archive
media drives, configuring . . . 67
media tasks . . . 66
log
manager . . . 30
viewer configuration . . . 32
logs
clearing . . . 211
exporting, component . . . 208
logs, application . . . 30
lost calls, finding . . . 236

M

manage tags . . . 103
managing agents . . . 224
media devices, managing . . . 217
media drives, local archive, configuring . . . 67
media tasks, local archive . . . 66
MIB, SNMP traps . . . 202
mixed codecs (IP only) . . . 84

N

named pipes, CTI Studio . . . 225
network
cards and filters . . . 159
protocols . . . 165
network settings
analyzer . . . 175
cards and filters . . . 159
protocols . . . 165
NGX voice cards
channel identifiers . . . 141
channels . . . 139
modifying . . . 135
NMS, SNMP traps . . . 202
Nortel Meridian/Succession via MLS . . . 290
Nortel Meridien/Succession via CTConnect . . . 288
notification profiles, alarms . . . 196

O

observer
column mapping . . . 97
configuring for live monitor . . . 98
ordering of columns . . . 104
Oracle maintenance . . . 228

P

parallel archive mode . . . 66
password, resetting . . . 30
pcap, winpcap filters . . . 159
PCM32 voice cards
channel identifiers . . . 134
channels . . . 132
modifying . . . 130
performance, checking . . . 235
postgres database maintenance . . . 230
preferences
analyzer . . . 176
user . . . 21
profiles, alarm, assigning . . . 188
protocols
E1 voice cards . . . 128
T1 voice cards . . . 127
protocols, network . . . 165
pruning contacts . . . 225
PWE3 . . . 159

R

reboot . . . 219
recorder
call buffer . . . 62
checking performance . . . 235
cloning . . . 227
components . . . 46
consolidator . . . 79
disk manager . . . 77
duplicating/cloning . . . 227

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

- license . . . 23
- local archive . . . 66
- rebooting and restarting . . . 219
- recording mode . . . 86
- screen recording . . . 105
- start and stop . . . 59
- status . . . 47
- troubleshooting updates . . . 65
- viewing status . . . 47
- voice cards . . . 111

recorder group
- creating . . . 179
- editing . . . 180

recorder manager
- audit logs . . . 238
- user administrator, add . . . 28

recording mode
- default, setting . . . 86
- extensions . . . 86

record, recorder recording mode . . . 86
related topics, help . . . 35
remote archive
- composite query template . . . 108
- rule . . . 108

resetting user password . . . 30
restart . . . 62, 219
restoring configuration information . . . 207
restrictions, live monitor replay . . . 104
rule . . . 108

S

SCCP . . . 165, 166
screen capture Recorder agent host diagnostics tool . . . 257
screen capture Recorder media channel diagnostics tool 257
screen recording . . . 105
security
- archive encryption . . . 69
- finger printing . . . 63
- tamper proofing . . . 259

sequential archive mode . . . 66
serial number . . . 224
settings
- alarm notification . . . 196
- alarms . . . 185
- call buffer . . . 62
- disk manager . . . 77
- recorder . . . 62
- screen recording . . . 62
- voice card . . . 111

silence an alarm . . . 191
SIP . . . 165, 166
sizing for live monitor . . . 95
SMTP . . . 176
SNMP . . . 176
- about . . . 202
- configure . . . 204
- creating and editing nodes . . . 203
- deleting . . . 204
- viewing nodes . . . 202

start and stop
- analyzer components . . . 174
- editing settings . . . 61
- rebooting and restarting . . . 219
- recorder and components . . . 59

status
- capture . . . 52
- Integration Service . . . 54
- other . . . 57
- thresholds . . . 50

status, checking . . . 235
status, recorder . . . 47
stop and start recorder and components . . . 59
swapping the system database . . . 228
switch report . . . 237
synchronization, voice cards . . . 234
system database, swapping . . . 228
system files . . . 30
system logs
- log manager . . . 30
- viewer configuration . . . 32

system maintenance
- add archive device . . . 214
- adding extensions . . . 225
- backing up . . . 226
- checking voice cards . . . 233
- disk management . . . 222
- duplicating recorders . . . 227
- finding lost calls . . . 236
- manage media devices . . . 217
- Oracle . . . 228
- postgres database . . . 230
- pruning contacts . . . 225
- rebooting and restarting . . . 219
- replace hard drive . . . 216
- restoring . . . 226
- serial number, changing . . . 224
- swapping databases . . . 228
- voice card . . . 215
- wiring, checking . . . 234

T

tags
- live monitor . . . 103

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.

voice card . . . 119
tamper proofing
correcting from CLI . . . 261
correcting with RM/EM . . . 259
thresholds, edit status summary . . . 50
trace logs . . . 238
transport protocol, CTI Studio . . . 225
troubleshooting . . . 238
component updates . . . 65
live monitor . . . 105
switch report . . . 237
TDM SCN diagnostics tools . . . 257
voice cards . . . 152
trunks
E1 protocol . . . 128
T1 protocol . . . 127
tutorial
Call Manager, active recording . . . 166
channel assignment . . . 155
VOX . . . 157
T1, modifying protocol . . . 127
T1/E1 voice cards
channels . . . 125
modify . . . 122

U

Unify
add extensions . . . 225
screen recording . . . 106
script, upgrading . . . 222
update personality, Cybertech voice cards . . . 148
user administrator, adding . . . 28
users
adding . . . 28
analyzer, managing . . . 176
creating . . . 27
deleting . . . 30
editing . . . 29
password . . . 30
preferences . . . 21
viewing authorized . . . 27

V

Viewer audit logs . . . 238
voice cards
adding . . . 115
add, wiring . . . 234
analog . . . 149
channels, viewing . . . 117
checking, system maintenance . . . 233
compatible types . . . 242
compression, Cybertech . . . 84
copying configuration . . . 113
Cybertech . . . 142
deleting . . . 114
editing tags . . . 119
E1, modifying protocol . . . 128
framer errors . . . 234
identifying . . . 113
modifying properties . . . 117
move, wiring . . . 235
NGX . . . 135
PCM32 . . . 130
remove, wiring . . . 235
replace, wiring . . . 234
replacing . . . 116
serial number . . . 111
setting up . . . 111
synchronization (framer) . . . 234
system maintenance . . . 215
troubleshooting . . . 152
T1, modifying protocol . . . 127
T1/E1 . . . 122
update personality, Cybertech . . . 148
updating channel configurations . . . 118
viewing . . . 111
VOX tutorial . . . 157

W

web services, restart . . . 62
winpcap, IP filters . . . 159
wiring, checking . . . 234

© 2005 - 2008 Verint Systems Inc. Confidential and Proprietary Information of Verint Systems Inc. All rights reserved, worldwide.